ISRAEL and the CYBER THREAT

How the Startup Nation Became a Global Cyber Power

CHARLES D. FREILICH, MATTHEW S. COHEN, and GABI SIBONI

Israel and the Cyber Threat

Israel and the Cyber Threat

How the Startup Nation Became a Global Cyber Power

CHARLES D. FREILICH,
MATTHEW S. COHEN, AND GABI SIBONI

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trade mark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.

Library of Congress Cataloging-in-Publication Data
Names: Freilich, Charles D. (Charles David), author. |
Cohen, Matthew S., author. | Siboni, Gabi, author.
Title: Israel and the cyber threat : how the startup nation became a global cyber power /
Charles D. Freilich, Matthew S. Cohen, Gabi Siboni.
Description: New York, NY : Oxford University Press, [2023] |
Includes bibliographical references and index.
Identifiers: LCCN 2022038833 (print) | LCCN 2022038834 (ebook) |
ISBN 9780197677711 (hardback) |
ISBN 9780197677728 (epub) | ISBN 9780197677742 (online)
Subjects: LCSH: Cyberspace operations (Military science)—Israel. | Cyber intelligence (Computer security)—Israel. |
Cyberspace—Government policy—Israel. | Cyberterrorism—Israel—Prevention. |
Cyberinfrastructure—Israel. | National security—Israel.
Classification: LCC U167.5.C92 F74 2023 (print) | LCC U167.5.C92 (ebook) |
DDC 355.4/75694—dc23/eng/20221020
LC record available at https://lccn.loc.gov/2022038833
LC ebook record available at https://lccn.loc.gov/2022038834

DOI: 10.1093/oso/9780197677711.001.0001

Printed by Sheridan Books, Inc., United States of America

CONTENTS

FIGURES, TABLES, AND MAPS

Figures

Table

Maps

ACKNOWLEDGMENTS

We wish to warmly thank a number of people for their invaluable support for this book, without which it would never have been written, certainly not at its current level of quality.

First, Prof. Eviatar Matania, the founding Head of the Israel National Cyber Directorate and current Director of the Security Studies Program at Tel Aviv University, for his professional guidance in writing this book and for the repeated interviews he granted us. His own book on Israel and cyber, which came out fortuitously just as were concluding ours, was an invaluable source.

We were extraordinarily fortunate to have had high-level access to many if not most of the senior officials involved in Israel's civil and military cyber realms in recent years. A list of interviewees is attached in the book's appendix. The list is far too long to thank each and every one of them individually, but we are truly grateful that they shared our belief in the importance of the book and were so very generous with their time.

Thanks to Professors Graham Allison and Stephen Miller, respectively director of the Belfer Center at Harvard's Kennedy School and director of the International Security Studies Program, under whose auspices much of the work for this book was conducted, and to the former head of the center's Cyber Security Program, Michael Sulmeyer, for financial support. Thanks to Dr. Gary Samore, director of the Crown Center at Brandeis, for his friendship and for the center's warm help in the final months of the book's writing.

We hope that the two unnamed book reviewers for Oxford University Press will find some compensation for the anonymity of their selfless work in the knowledge that their extraordinarily insightful comments greatly changed the quality of the manuscript for the better.

We are indebted to a number of people who read and commented on various chapters, including Dr. Lior Tabanksy, Dr. Deganit Paiowsky, Dr. Amit Sheniak, Lior Yafe and, once again, Eviatar Matania. We are also indebted to a number of

former students who helped with the research at different stages of the process, including Saskia Becaud, who was a collaborator on a number of projects, Daniel Sorek, Jeremy Staub, Brit Felson Parsons, and Jacob Fortinsky. Gal Sapir also provided research assistance.

Our thanks to Dave McBride, Social Science Editor at Oxford Press for shepherding the manuscript through a long gestation period, Emily Mackenzie Benitez, Senior Project Editor at Oxford Press, Suganya Elango, Production Manager, and Bríd Nowlan, copy editor.

Finally, although most certainly not least, we wish to express our deepest thanks and appreciation to our parents, wives, and children, to whom this book is dedicated. For Chuck—Anne and Ted, Idit, Lior, and Tal. For Matthew—Bruce and Marian, Julie, Brianna, and Ben. For Gabi—Liat, Ofer, Noam, and Yotam.

AUTHOR BIOS

Prof. Charles ("Chuck") Freilich, a former deputy national security adviser in Israel and long-time senior fellow at Harvard's Belfer Center, teaches political science at Columbia, New York, and Tel Aviv Universities. He is the author of *Zion's Dilemmas: How Israel Makes National Security Policy* (Cornell University Press, 2012) and *Israeli National Security: A New Strategy for an Era of Change* (Oxford University Press, 2018 and Modan Press in Hebrew). Chuck is the senior editor at the Israel Journal for Foreign Affairs, has published numerous academic articles and over 170 op-eds, and appears frequently on US, Israeli, and international TV and radio stations. He earned his PhD from Columbia University.

Prof. Matthew S. Cohen earned his PhD in political science at Northeastern University. He currently serves as an Assistant Professor of Practice at Merrimack College. Matthew's research is focused on emerging security threats. He has published on cyberspace, international relations theory, Israeli security policy, delegitimization and lawfare, Turkish-Israeli relations, Turkish politics, and Russian politics.

Prof. Gabi Siboni, a former colonel in the IDF, is a senior research fellow at the Jerusalem Institute for Strategy and Security and a consultant to the IDF and other Israeli defense organizations, including as the chief methodologist of the IDF's Research Center for Force Deployment and Buildup. Gabi was the director of both the Military and Strategic Affairs and Cyber Security Programs at the Institute for National Security Studies (INSS) and also edited the institute's academic journals in these areas. Gabi earned his PhD in Geographic Information Systems from Ben-Gurion University and has published numerous academic and other works on national security and cyber security affairs.

ABBREVIATIONS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATP	Advanced Technology Park
CBM	Confidence Building Measure
CEC	Cyber Education Center
CERT	Computer Emergency Response Team
CNA	Computer Network Attacks (for purposes of disruption or destruction)
CNE	Computer Network Exploitation (cyber espionage)
CNI	Computer Network Influence (cyber information operations)
CT	Counterterrorism
CWC	Chemical Weapons Convention
DDoS	Distributed Denial of Service attacks
DMP	Decision-Making Process
DoD	(US) Department of Defense
DoS	Denial of Service attacks
GUCD	Governmental Unit for Cyber Defense
IAF	Israel Air Force
ICT	Information Communications Technology
IIA	Israel Innovation Authority
IISS	International Institute for Strategic Studies
INCD	Israel National Cyber Directorate
INSC	Israel National Security Council
INSS	Institute for National Security Studies

IoT	Internet of Things
IRGC	Iranian Revolutionary Guards Corps
ISA	Israel Security Agency, also known as the Shin Bet or Shabak
JCPOA	Joint Comprehensive Plan of Action ("Iran nuclear deal" 2015).
LOAC	Law of Armed Conflict
MABAM	campaign between the wars (Hebrew acronym)
MI	Military Intelligence
MNC	Multinational Corporation
MoD	Ministry of Defense
MoU	Memorandum of Understanding
NCSA	National Cyber Security Authority
NCSC	National Cyber Security Center
NISA	National Information Security Authority
NIW	(Iranian) National information network
NPT	Nonproliferation Treaty
NSA	(US) National Security Agency
NSC	(US) National Security Council
NSS	National Security Staff (new name for INSC above)
SOC	Security Operations Center
UAE	United Arab Emirates

PROLOGUE

It was a quiet summer evening when the first signs of trouble appeared. Some people in Tel Aviv were already strolling on the beachfront promenade, others were still caught in rush hour traffic. Suddenly, traffic lights went out and within minutes central Israel became one big snarl. In Jerusalem, an ambulance with a patient in cardiac arrest was unable to reach Hadassah hospital. The radar at Ben-Gurion Airport went blank and aircraft had to be diverted to Cyprus.

Soon electricity began sputtering around the country. Air conditioners and computers shut off, and hot and increasingly irritable people began wondering what was going on. Young techies at Microsoft, Facebook, and other high-tech firms were particularly exasperated. In Dimona, the usually well-lit security fence around the nuclear reactor was shrouded in darkness.

Banking services crashed, and many found that their accounts and investment portfolios registered a zero balance. TV programs were disrupted, but soon showed images of Israelis killed in terrorist attacks. Social media were overwhelmed by vicious propaganda messages, and phone communications collapsed.

It was then that a barrage of Hezbollah rockets began hitting population centers, airbases, and other major military targets. Some people noticed that Iron Dome, Israel's vaunted anti-rocket system, seemed to be missing its targets. Unbeknown to them, Iron Dome operators were frantically trying to recalibrate their unresponsive computers. An air force pilot reported seeing extensive troop movements along the northern border, but monitoring systems gave no indication thereof.

Tensions had been building for months. Iran was closer than ever to a nuclear breakout and now had a forward operating base in Syria from which to attack Israel, in addition to the 130,000 Hezbollah rockets housed in Lebanon.

Over the next few days, the IDF mobilized reserves. Many never received the messages sent to their smartphones. Others did, but were caught in the never-ending traffic. By the time their units were able to fully mobilize and reach the front . . . .

This account is based on actual events and IDF training scenarios, with just a little help from our imaginations.[1]

Introduction

Cyber winter is coming and coming even faster than I expected.
Yigal Unna, Head of Israel National Cyber Directorate, 2020

Cyber winter is here.
Yigal Unna, Head of Israel National Cyber Directorate, 2021

Israel has the world's most tech-dependent economy and is a global leader in high-tech R&D and startups, per capita. Israel has also come to be a leading cyber power, home to as many cyber startups as the rest of the world combined, not including the United States. Israel is also widely considered a leading actor in both defensive and offensive cyber capabilities, and its overall cyber prowess has become an important component of its national security. As such, the cyber realm has come to constitute a truly remarkable boon for Israel and a critical dimension of every aspect of its national life today—socioeconomic, cultural, governmental, diplomatic, and military.

For Israel's enemies, conversely, its dependence on the cyber realm is also a potential source of weakness, making it more vulnerable to cyber attack than they and providing a possible means by which to counter Israel's economic power and military superiority.[1] Israel has thus become one of the top targets of cyber attacks in the world today, facing a nearly constant daily barrage, both by state and nonstate actors. Indeed, cyber attacks have come to be viewed as one of the primary threats that Israel faces today.[2]

Attackers have targeted virtually every type of computer system in Israel, hospitals, El Al airline, the Tel Aviv Stock Exchange, Bank of Israel, and television stations, to mention just a few.[3] Critical infrastructure firms, providing electricity, water, communications, and more, have been a particular focus of attack. The Israel Electric Corporation (IEC) alone typically faces hundreds of thousands of attacks every day. Most are mere nuisances and easily deflected, but some are sophisticated efforts to disable its systems. A successful cyber attack on the IEC could disrupt power to virtually all of Israel and paralyze the

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0001

nation, with potentially severe civil and military consequences. In 2020, a cyber attack on Israel's water system was detected before dangerous levels of chlorine could be released into the national supply.[4]

Most of the known attacks are against purely civilian targets and are designed simply to cause disruption and hardship. Some are conducted without any stated political agenda or set of demands and are offshoots of wider campaigns aimed at undermining Israel's international standing, weakening it physically, and undermining its societal resilience. For years, on the eve of Holocaust Remembrance Day "hacktivist" groups have conducted a coordinated annual series of cyber attacks against Israeli websites. One such group has repeatedly threatened Israel with an "electronic Holocaust" and of being "erased" from cyberspace.[5]

In 2019 foreign hackers almost succeeded in inserting fake video footage, purporting to show rockets raining down on Tel Aviv, into the televised broadcast of the Eurovision Song Contest, an annual musical extravaganza held that year in Israel and viewed live by hundreds of millions of people around the world. In 2020 hackers from Iran, China, North Korea, Russia, and Poland launched more than 800 cyber attacks against Ben-Gurion airport and approaching aircraft, to disrupt the arrival of more than 60 world leaders attending a commemoration of the 75th anniversary of the liberation of Auschwitz, including the presidents of Russia and France and the US vice president. In 2022 hackers sought to disrupt President Zelenskyy's live address to the Knesset, at the height of Ukraine's war with Russia.[6] Had any of these attacks succeeded, the damage to Israel's image, tourist industry, and commercial sector, as a whole, would have been severe.

Israel faces a myriad array of military threats and relies for its security on a largely reservist army with exceedingly short mobilization times. A cyber attack that successfully disrupted power, communications, or transportation systems, even for a short period, could make a critical difference in times of crisis or war. Even something as basic as shutting off traffic lights or disrupting cellular communications could delay the mobilization of forces and have a significant impact on military operations, not to mention the chaos caused to the entire country. Attacks that successfully penetrated command-and-control and intelligence systems, or even weapons systems, could have an even more severe impact.

Iran, Hezbollah, and Hamas, unsurprisingly, are the primary sources of cyber attacks against Israel. Iranian hackers reportedly targeted Israeli nuclear scientists with "phishing" scams in an effort to gain access to sensitive information.[7] An Iranian-affiliated website succeeded in causing a brief, but dangerous, spiral in tensions with Pakistan, based on an entirely fabricated nuclear threat that Israel had supposedly made and a real nuclear threat that Pakistan made in response.[8]

Iran, Hezbollah, and Hamas have apparently used Facebook and messaging apps for purposes of terrorism against Israel.[9] Palestinian Islamic Jihad hacked

the (unencrypted) communications of IDF drones operating over Gaza, thereby gaining real-time intelligence that enabled it to better hide its rockets from Israeli strikes.[10] Hamas hackers, posing as attractive Israeli women, enticed IDF soldiers into downloading fake dating sites onto their smart phones. In so doing, they were able to gain control over the soldiers' phones, overhear the operational briefings they attended, or film their bases and military positions. Even when the soldiers used secure land lines for operational purposes, the infected phones continued to transmit what they were saying.[11]

Cyber attacks against Israel do not only originate with its Middle Eastern adversaries.[12] Much like the United States and other democratic countries today, Israel is also concerned about attempts to subvert its electoral system and influence public opinion through cyber means.[13] Russia and China and their cyber espionage are a particular source of concern,[14] as are even close allies. During a high point in Israel's ongoing conflict with Hamas in Gaza and, even more importantly, at a time when Israel was preoccupied with the danger of a possible Iranian nuclear breakout, US and British intelligence reportedly tapped into live video feeds from Israeli aircraft, monitored military operations in Gaza, and watched for a potential strike against Iran.[15]

As seen in Figure I.1, the incidence of cyber attacks increases markedly during both major diplomatic developments and military crises.[16] During the 2009 conflict with Hamas, four waves of progressively stronger attacks were launched.[17] The Home Front Command's website, a critical means of communicating with the public during military emergencies, including instructions on protective measures to be taken during rocket attacks, was temporarily taken off-line.[18] During the 2012 conflict, major commercial and governmental websites were disrupted, including the Prime Minister's Office and Foreign and Defense ministries,[19] and TV broadcasts were briefly replaced with Hamas propaganda films.[20] During the 2014 conflict, Iranian hackers reportedly attempted to seize control of Israeli drones[21] and in 2018 to disrupt the Home Front Command's rocket defense systems. Had they succeeded, they would have been able to declare false alerts, or even worse, prevent the national alert system from being operated and disrupt defenses against incoming rockets.[22]

A dramatic upturn in Iranian cyber attacks against private Israeli firms took place in 2019–2021. One attack, against an insurance company that caters largely to defense establishment employees, led to a dump on the Internet of their names, the sensitive organizations they worked for, phone numbers, home and email addresses, credit card numbers and more, a veritable gold mine of information for foreign intelligence services.[23]

The cyber threat to Israel is, of course, just a small part of the far broader global information revolution. The numbers are staggering. The world now creates as much data in two days today as it did from the dawn of time up to

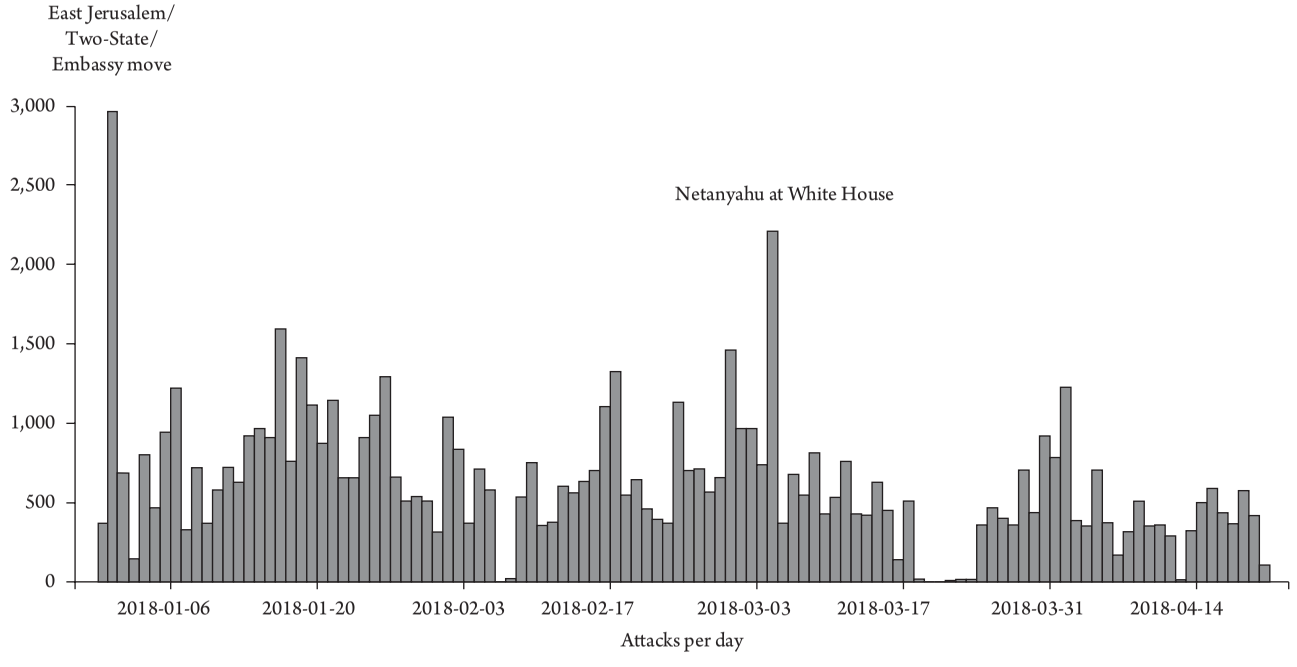


Figure I.1 Malware Peaks and Political Developments Source: Adapted from Kausch and Tabansky 2018.6

2003. By 2012, 90% of all data ever produced by humanity had been created in the previous two years. The amount of data created in 2020 was estimated to be fifty times greater than that in 2016.[24] The number of home computers around the world has long since passed the 2 billion mark, some 5 billion people own a mobile phone and more than 20 billion devices are thought to be connected to the Internet, a number that will expand rapidly with the spread of the Internet of Things (IoT)[25] and Internet of Body (IoB).* Each computer and phone represents a change in the global lifestyle but can also serve as an entry door for malicious cyber activity. It is thus hardly surprising that the World Economic Forum has ranked large-scale breaches of cyber security as one of the five most serious risks facing the world.[26]

The exponential power of information networks—and consequently of information operations—is shown in Figure I.2. Whereas two telephones are needed to make one connection, five telephones will make ten connections, twelve will make sixty-six connections and so on.[27]

Between 2005 and 2019 more than 11.5 billion records containing personal data, mostly of US citizens, such as email addresses and social security numbers, were stolen in over 9,000 separate cyber attacks. During 2017–2019 alone, personal data was stolen from the accounts of nearly 140 million Facebook, 57 million Uber, 100 million Capital One, and 143 million Equifax users. Perhaps most embarrassingly, 400 million users of the Adult Friend Finder, a casual sex site, were also compromised.[28]

One report estimated the cost of global cyber crime in 2018 at $600 billion, an increase of $100 billion over 2014, and forecast that it would reach a whopping $6 trillion by 2021. US firms lose roughly $250 billion each year as a result of cyber theft of intellectual property. The damage from a successful cyber attack against just one of the operators of the US electric grid has been estimated at anywhere between $240 billion and $1 trillion.[29]

Ransomware attacks, in which the target is forced to pay a fee in exchange for a digital key that unfreezes a maliciously encrypted system, have become one of the most important forms of cyber crime, and one which is increasingly viewed as a national security threat. In 2020 global ransomware attacks nearly doubled. In 2021 they took place in the United States alone, on average, every eight minutes. Russian groups are believed to be behind most ransomware attacks to date, although direct governmental complicity has yet to be fully established.[30]

Various state actors, including Russia and Iran, have planted, or at least planned, intrusions on the US electric grid, as the United States has on theirs,

* The IoT refers to home appliances, autonomous vehicles, transportation, manufacturing and agricultural systems, and more. The IoB is an extension of the IoT that connects the human body to computer networks through devices that are ingested, implanted, or connected to it.

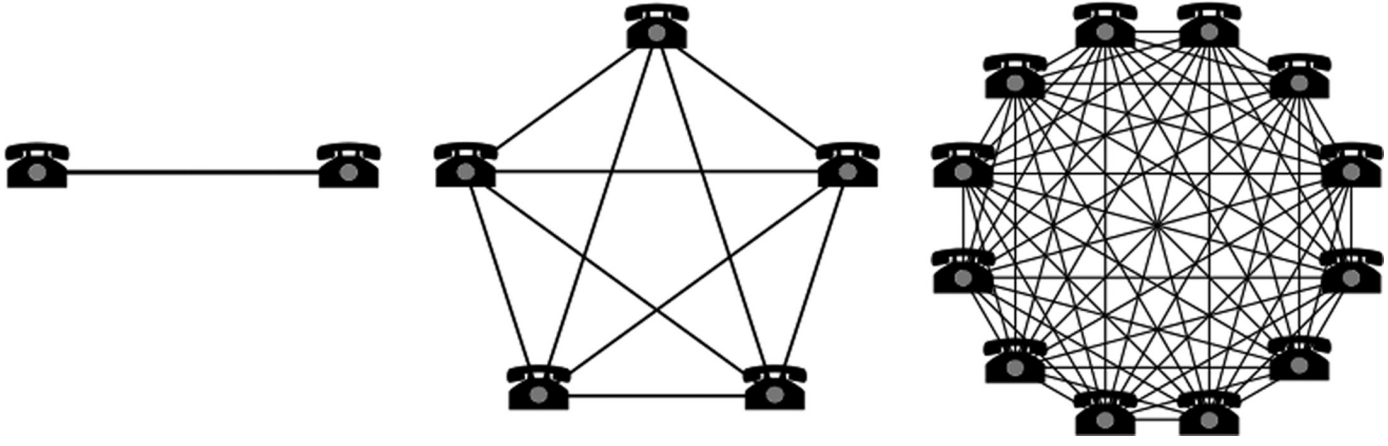


Figure I.2 Metcalf's Law Source: BeanLabs.com

or China has on India's.[31] In 2021, the computer systems of a water treatment facility in Florida were breached, raising fears that dangerous chemicals could have been released into the water supply.[32] These and other attacks on critical national infrastructure, with potentially systemic effects, are a particularly severe danger.

In 2020 hackers sought to steal information about Covid-19 vaccine research in the United States, UK, Canada, and elsewhere. Chinese-affiliated attacks apparently began within months of the pandemic's outbreak, followed by Russian and North Korean attacks. Spearfishing emails impersonated executives at legitimate firms involved in the global vaccine distribution chain, as well as representatives of the World Health Organization (WHO) and personnel recruiters for pharmaceutical companies. Confidential information regarding the Pfizer vaccine was stolen from the European Medicines Agency, the regulatory agency responsible for authorizing its use throughout the EU. UNICEF, which was planning vaccine delivery for poorer countries, was apparently also the focus of an attack.[33]

Cyber poses a particularly severe threat in the military realm. Were an attacker able to shut down an adversary's electric grid, for example, it would be possible to bring both its economy and military to a virtual standstill and conceivably have a decisive impact on the outcome of a conflict. Cyber attacks might render certain weapon systems inoperable, or inaccurate. Most future military engagements of any magnitude are likely to include at least some cyber operations.[34]

Russia may have been the first state to conduct cyber campaigns designed to achieve strategic effects and destabilize foreign governments. Russian operations began with attacks against Estonia in 2007, subsequently dubbed Web War 1.[35] A year later, during a conflict with Georgia, Russia combined ground and air attacks with cyber operations. Starting in 2014, Russia merged conventional and cyber means into a continuous form of hybrid warfare designed to prevent Ukraine from contesting the annexation of Crimea and occupation of the eastern part of the country. The 2017 NotPetya cyber attack on Ukraine's government, power grid, and banking system may have been the most costly and destructive ever. Speculation was rampant in 2022 that Russia would preface an invasion of Ukraine with widespread cyber attacks.[36]

China considers cyber a particularly effective means of conducting deniable, asymmetric warfare[37] and has successfully hacked blueprints and plans for major US weapons.[38] For North Korea, the cyber realm is a cheap means of attempting to level the playing field with the United States and one in which it can act with virtual impunity, given the undeveloped nature of its own cyber infrastructure. In 2015 North Korea launched widespread cyber attacks against South Korean banks and broadcasters, paralyzing roughly 48,000 computers as well as a nuclear energy firm, raising concerns regarding the safety of South Korea's power

plants. In 2016 North Korea successfully breached a South Korean military computer system that contained detailed US war plans and began using cyber crime as a means of financing its nuclear and missile programs. In 2017 it launched WannaCry, a severe ransomware attack that spread to 230,000 computers in nearly 100 countries, starting with the British National Health Service.[39]

The United States is one of the most aggressive actors in the military cyber realm and openly declares its intention to dominate it. As early as 2013, the United States had already breached over 85,000 computer systems in 89 countries, reportedly including China's national and nuclear command and control systems, and implanted malware in Russia's electric grid. The United States sought to sabotage North Korea's missile program and has conducted a number of cyber attacks against Iran, including the Stuxnet attack on its nuclear program, implants in its computer networks in preparation for possible preemptive strikes, and attempted sabotage of its missile program.[40] In response, Iranian hackers attacked 46 major US financial institutions, forcing them to spend billions of dollars on cyber security. In a particularly destructive cyber attack, they also targeted Aramco, the Saudi national oil company, bringing it to the verge of collapse.[41]

Cyber has had a dramatic impact on espionage operations. In 2020, 18,000 customers around the world downloaded Russian malware, including tens of high value targets mostly in the United States, such as the National Security Agency and National Nuclear Security Administration (which maintains the US nuclear stockpile), but also in Canada, Mexico, the UK, Belgium, Spain, the UAE—and Israel.[42] Whereas intelligence agencies in the past had to go to great lengths to gain access to just a single such target, the scope of the Russian attack and potential for damage were staggering. In 2020 Chinese hackers breached the Vatican's email system to gain intelligence regarding its positions on negotiations over the controversial appointment process of Catholic bishops in China.[43] At the height of the negotiations with the United States that ultimately led to the nuclear deal in 2015,[†] Iran breached the personal email accounts of the US negotiating team, other US officials, and Congressional critics of Iran.[44]

The cyber realm has also become an instrument of social control at home and a means of achieving economic advantage abroad. China has built the "Great Firewall of China" to control what domestic users can access on the Internet and to spy on them. It has also conducted extensive cyber operations against technology firms and financial institutions in the United States, Japan, and Europe. State-linked Chinese firms, using AI, facial recognition software, and cell phones, are building a global mass surveillance capability against political opponents.[45]

[†] The Joint Comprehensive Plan of Action (JCPOA).

Russia is centralizing domestic Internet traffic and creating chokepoints designed to seal it off from the rest of the world.[46] Iran, too, has developed a national intranet to control access. An Iranian cyber surveillance campaign during 2014–2020, reportedly capable of outsmarting encrypted messaging systems, spied on dissidents and minorities at home and abroad.[47]

Cyber information operations, especially against elections in Western countries, have proven a particularly effective instrument of power. In 2008 China hacked the presidential campaigns of Barack Obama and John McCain and that of Joe Biden in 2020.[48] Russia's attack on the US presidential elections in 2016 was arguably the most prominent cyber attack ever, certainly the most prominent cyber information campaign. It may have also been part of a broader strategy designed to split the Western camp, weaken NATO, and erode public faith in Western democracy and institutions in 19 countries. Initially designed to embarrass Hillary Clinton and undermine her public stature, the Russian campaign appears to have evolved into an attempt to sway the election in favor of Donald Trump. Russian interference in US elections continued, albeit at a lower level, in 2018 and 2020.[49]

Iran has interfered in US elections ever since 2012. In 2016 Iranian hackers sought to boost the presidential campaign of Bernie Sanders, who was considered more favorable to their interests than the Democratic front runner, Hillary Clinton. In 2020 Iran hacked both the Trump and Biden campaigns, in an attempt to sway the outcome in the latter's favor and prevent the reelection of its nemesis, Trump. In an attempt to promote further discord following the elections, an Iranian-affiliated website issued death threats against those US elections officials and governors who had refuted the claims of voter fraud. Other Iranian information operations sought to leverage domestic controversies, such as the Black Lives Matter movement, to further exacerbate tensions in the United States.[50]

As with other exciting new technologies, there is much hype surrounding the threats and opportunities posed by the cyber realm, some warranted, some not. Cyber certainly does not change everything and, in many important ways, the threat it poses is not fundamentally different from older and better-known asymmetric capabilities, such as terrorism or chemical and biological weapons. Much as there are no air-tight solutions to these threats, there will be none to cyber either.

States have, however, learned to cope with the dangers and to reduce them to levels that do not usually impose unacceptable costs on their ways of life. Subsequent chapters will show that many of the same policy considerations that apply to other asymmetric threats, and to the physical realm as a whole, are also applicable to the cyber realm and that the fundamental principles of military strategy will remain largely unchanged. Nevertheless, cyber does pose critical new challenges to states' national security. Major new capabilities have

emerged, and will continue to emerge, that are sufficiently different from existing capabilities to warrant the special attention afforded to the cyber realm by theoreticians and practitioners alike, this book included.

Why Study Israel?

Segal argues that the strongest cyber powers have four common characteristics: larger, technologically advanced economies; public institutions that channel the energy and innovation of the private sector; adventurous military and intelligence agencies; and an attractive story to tell about the cyber realm.[51] Israel is certainly an outlier among the other top cyber powers, the United States, China, Russia, and the UK. Its economy is far smaller, and it is, of course, a regional actor not a global power. Nevertheless, Israel does generally meet Segal's criteria. In the cyber realm and in high tech generally, Israel has an outsized and advanced economy. Its public institutions, both civil and military, play an unusual role in channeling the energy and innovation of the private sector. Israel's military and intelligence services are highly advanced and forward-looking and have played a critical role in developing Israel's high-tech and cyber capabilities. Lastly, as this book seeks to demonstrate, Israel certainly has an attractive story to tell in the cyber realm.

Israel was one of the first states to awaken to the cyber threat and to respond by developing capabilities that have placed it today at the forefront of the cyber realm. As early as 2012, a comprehensive study examining the preparedness of states in the cyber realm accorded Israel the highest ranking. Over time, Israel's cyber policy and practices, including the governmental agencies and ecosystem it has established, have come to be considered global trend setters.[52] Israel is also thought to be one of the more active states in the military cyber realm and to be a world leader in both cyber offense and defense.[53]

In 2021 the International Institute for Strategic Studies (IISS), a prestigious British think tank, ranked Israel as one of the states in the second tier of global cyber capabilities, flatteringly grouped together with the UK, Russia, and China, just one notch below the first-tier United States. According to IISS, Israel and the UK were at the top of the second tier in terms of cyber security, intelligence, offense, and international alliances, but behind Russia and China in terms of human and financial resources, unrestrained operational boldness, and experience conducting cyber information operations. It further found that Israel benefits from clear political direction in the cyber realm, a whole of society approach, and a vibrant and innovative startup ecosystem.[54]

Israel's experience is thus of significance for both academic experts and practitioners who are interested in the ramifications of the changes that the

cyber realm has wrought, the theoretical quandaries in the cyber literature, and practical questions of cyber strategy. The Israeli cyber story is fascinating in its own right, but it is Israel's ability to serve as an experimental test site and model for other states that makes it especially worthy of study. Israel has long been a laboratory and harbinger of things to come in national security affairs, studied by experts and governments around the world. All states have their own particular strategic, institutional, and political settings, but the lessons and conclusions that can be derived from the Israeli experience offer useful insights that can be adapted to their requirements.

The existing literature on Israel and the cyber realm is limited, both in quantity and breadth, with most works focusing on specific aspects of Israeli cyber policy and practice. One of the earliest treatments of Israeli cyber policy, by Even and Siman-Tov (2012), addressed the institutional arrangements existing at the time, as well as some of the capabilities Israel had developed. Baram (2013) and Parmenter (2013) studied the implications of cyber weapons for IDF force buildup and military strategy generally. The most comprehensive study of Israel and cyber security to date, by Tabansky and Ben-Israel (2015), touched on many of the salient issues at the time, but was unfortunately brief and is now dated.

A number of authors have traced the evolution of Israel's cyber strategy. Siboni and Assaf (2015) proposed a number of "guidelines" for a national cyber strategy, arguing that the overriding objective should be to maintain the functional continuity of the state, even under severe attack. Cohen and colleagues (2016) set out some of the basic arguments that are fleshed out in far greater detail in this book. Raska (2015) provided a good general overview of Israel's cyber strategy, to which Housen-Couriel (2017) added some further detail. Baram (2017) stressed that technology has always had a place of prominence in Israel's national security thinking, as a means of maintaining a qualitative edge over Israel's larger and quantitively superior adversaries. He further argues that Israel has been able to integrate the cyber realm into the fundamental pillars of its classic defense doctrine: deterrence, early warning, defense, and decisive victory.[55] Adamsky (2017) provided one of the earliest accounts of the strategy formulated by Israel's National Cyber Directorate (INCD).

Other authors have focused on the institutional arrangements and the ecosystem that Israel developed in order to implement its evolving cyber strategy. Benoliel (2015) described the work of the INCD, outlining its functions and offering suggestions for further improvement. Tabansky (2020) and Frei (2020) offer more up-to-date descriptions of the evolution of Israel's strategy and institutional arrangements, including the most detailed accounts to date of the defense agencies involved. Tabansky stressed the importance of military human capital and the IDF's organizational culture for the civil cyber sector. Frei emphasized the rapid and efficient exchanges of information between Israel's

close and well-connected civil and military cyber ecosystem and the growing centralization of both Israel's civil and military institutions responsible for cyber security. Matania and Rappaport's (2021) insider account of the establishment of the INCD adds both important new information and much welcome color. Matania was the founding and two-term head of the INCD, and his perspective on the processes leading to its establishment, as well as some of the major cyber issues of our times, from both global and Israeli vantage points, are of considerable importance.

Siboni and Sivan-Sevilla (2017) studied Israel's approach to regulation as a model of how nations build resilience and reduce risk in the cyber realm. With the exception of critical national infrastructure, in regard to which the government has always taken an active role, they argue that Israel has taken a generally hands-off approach, relying on the market to find the appropriate balance between cyber security and commercial activity.

Much of the literature on Israel and the cyber realm has been devoted to the cyber attack on Iran's nuclear program, the Stuxnet virus, which has been widely attributed both to the United States and Israel. Zetter (2014) and Sanger (2012 and 2018) presented highly detailed accounts of Stuxnet, including purported US-Israeli cooperation in carrying it out. Many of the studies of Stuxnet and the Olympic Games cyber sabotage program, of which it was a part, have addressed the potential ramifications for the future of national security policy. Even and Siman-Tov (2012) and Parmenter (2013) argued that Olympic Games and Stuxnet signified a new era of cyber warfare, by demonstrating that a computer virus could be an effective covert means of causing physical damage to an adversary. As such, they and others maintain that these operations may have affected national doctrines regarding the offensive use of cyber weapons and even the way foreign relations and warfare are conducted.[56] Lindsay (2013), conversely, argued that these operations actually demonstrated the limits of cyber attacks, which pose highly complex technical challenges that make them difficult to conduct and only marginally increase the power of stronger actors. Israel's strike on a Syrian nuclear reactor in 2007, in which it allegedly employed cyber measures to blind Syrian defenses, has also been the focus of considerable interest.[57]

The Analytical Framework

Advanced technological capabilities, both civilian and military, have been at the heart of Israel's national security strategy and socioeconomic policy from the earliest days, even before independence. In the face of what Israel believed to be an existential threat stemming from its adversaries' quantitative military and economic superiority, advanced technological capabilities were considered

strategic and economic imperatives. Technological prowess was to be the basis for Israel's socioeconomic development, from its heavily agrarian and quasi-socialist beginnings, into a dynamic, modern economy. Socioeconomic development, in turn, was to be the basis for a qualitative military edge, based both on human resources of the highest caliber and highly advanced technological capabilities, including domestically produced weapons.[58] By the early 2000s Israel had become a leading international center of high-tech.

Cyber attacks posed a new and potentially severe addition to the array of conventional, unconventional, and mostly asymmetric threats that Israel faced from the 1990s on. Confronted with this emerging threat, Israel was an early adapter of cyber technology, developing some of the world's most advanced civil and military cyber capabilities in the process. As such, its initial response was a matter of sheer strategic necessity.

One would, however, be hard-pressed to think of a new technology better suited to Israel's national strengths and needs, including its already existing and highly advanced civil and military technological capabilities; the limited development and manufacturing costs required, compared to other industries; the need for only modest numbers of extremely talented and innovative scientific and technological personnel; and the potential for a relatively rapid but high return, both economically and in the crucially important military domain. As such, the response was a matter of strategic and socioeconomic opportunity, not just necessity.

Cyber was also particularly suited to the emphasis Israel's strategic culture had long placed on technological solutions to economic and military challenges, as well as to its overall national temperament—what we call chutzpah gone viral—in which accepted norms, practices, and sources of authority are constantly questioned, and improvisation, creativity, and innovation are highly prized values. Chapter 6 further elaborates on the impact of Israel's strategic culture and national security strategy, but these basic cultural predilections have fused over the years with the strategic and socioeconomic imperatives to improvise and innovate. In the process, they have become deeply ingrained, almost reflexive Israeli traits, a national modus operandi and sphere of excellence, often even when more established and routinized means may be preferable.[59] As such, the response was a domestic, cultural one, as well.

Israel's military and intelligence organizations—conservative and even hidebound establishments in most countries—are also deeply imbued with this innovative national culture and have become primary engines thereof, further promoting both technological and socioeconomic development generally. Indeed, the relationship between Israel's defense establishment and civilian cyber ecosystem is a symbiotic one, with each feeding into the other and further propelling their joint development.[60]

To put matters in social science terms, we posit that the independent (causal) variables of strategic and socioeconomic necessity and opportunity—working through the filter of strategic culture, an intervening variable that affected Israel's assessment of the options available to it—led to the development of Israel's highly advanced civil and military cyber capabilities, the dependent variable.

Needless to say, in the complex real-world decision-making processes surrounding the evolution of Israeli cyber policy, additional factors came into play at different times. Individual political leaders were quick to identify the importance of the cyber realm for Israel and to champion the development of its capabilities. Israel's public institutions, both civil and military, successfully channeled the energy and innovation of the private sector. Bureaucratic politics affected the evolution of Israel's civil cyber institutions and had a strong impact on the IDF's cyber force structure. Domestic politics affected the substance of Israeli cyber law and interfered with its development. We will address all of these and additional factors; all are important, but they are secondary to the primary independent variables set out above. To the extent that this is not found to be true, the hypothesis will not have been substantiated.

The independent variables derive mainly from the realist school of international relations theory. Realist scholars argue that the international system is dominated by a state of anarchy, which includes ongoing threats of violence, including war, meaning that states exist in a self-help world in which they must constantly strive to increase their national power, both military and economic, in order to survive.[61] The pursuit of power leads to a fundamental "security dilemma": when state A strengthens its capabilities in order to increase its security, state B feels threatened and does so as well, leading state A to strengthen its capabilities once again, and so on. An arms race and the consequent dangers of escalation ensue, even when states perceive their motivations and actions to be entirely defensive.[62] This constant state of anarchy and competition means that states are reluctant to cooperate or reveal their capabilities.

In the context of the cyber realm, the situation of pervasive systemic anarchy is such that states must strengthen their security by developing greater cyber power, including both offensive and defensive military capabilities, and drawing on a national cyber ecosystem. To counter the dangers to their security, states penetrate other states' computer systems and networks to collect intelligence on their capabilities, cyber and otherwise, or to disrupt and degrade them, thereby creating a "cyber security dilemma." The resulting cyber arms race may increase the risks of escalation, uses of force, and war.[63]

The security dilemma in the cyber realm is further exacerbated by some of its unique or at least particularly pronounced characteristics, including the absence of an established body of international norms and law, or a global regime, to moderate interstate conflict; the absence of geographic boundaries, meaning

that conflict can originate from and take place in any part of the world; the prevalent assumption that the cyber realm favors the offense and the difficulty in distinguishing between offensive and defensive cyber measures; and the unique character of cyber weapons, which makes states particularly hesitant to discuss their capabilities, because the very act of doing so can render them ineffective. Moreover, the very nature of the Internet, which was built around the idea of open access, not security, increases the difficulties states encounter in establishing a monopoly of force even over their domestic cyber realms.[64]

Some scholars challenge the inherently anarchical nature of the cyber realm, noting that countries such as China, Iran, and North Korea have been able to impose varying degrees of control over domestic and international Internet traffic. Democracies, too, have managed to assert a modicum of control and are not the helpless victims of a completely anarchic system.[65] Nevertheless, the basic observation remains appropriate, and these controls can be bypassed by determined state and nonstate actors. More to the point, there is considerable debate, both in the theoretical and policy oriented literature, about issues related to realist thought, such as the efficacy of cyber deterrence, whether cyber is more or less escalatory than other types of conflict, and whether defeat is even a relevant concept in the cyber realm. To illustrate, whereas the US and UK governments believe that the concept of deterrence is as applicable to the cyber realm as to the physical, theorists are more skeptical.[66] We will return to these quandaries in detail in Chapter 2.

Many believe that the cyber realm represents a fundamental change in the very concept of national power, both socioeconomic and military. Whether true, or not, there is no doubt that cyber has become an important source of economic power and a critical component of many states' defense postures. Indeed, cyber attacks have already been shown to have considerable effects, against both civil and military targets.[67] Realists also speak of the concept of creative insecurity, which may arise when two conditions apply: a state perceives significant external threats to its security, such as military invasion, or severe cuts to strategically important imports (e.g., weapons and natural resources); and this threat perception incentivizes scientific and technological innovation designed to foster and sustain an internationally competitive economy. The internationally competitive economy then yields the foreign exchange that states need to purchase strategic imports, or build domestic defense industries, thereby reducing their reliance on foreign suppliers.[68]

Realist thinking has certainly applied to Israel, which has been driven by a fundamental sense of insecurity stemming from an external environment that was, and in many ways remains, characterized by extreme hostility.[69] In keeping with realist arguments, Israel viewed advanced technological capabilities, including cyber, as the appropriate response to the strategic and socioeconomic

challenges it faced and has thus sought to increase its national power by building outsized civil and military cyber capabilities. Moreover, the very concept of creative insecurity is particularly applicable to Israel (see Chapter 6).

Constructivism offers a different view of the international order. Constructivists do not deny the anarchic nature of the international system and states' consequent need to pursue power in order to heighten their security. But they argue that it is states' self-identities and beliefs that are the primary determinants of their behavior on the international stage. State identities are social constructs, shaped by their self-perceptions, national cultures, histories, and beliefs regarding their strategic circumstances and interests, whether transient or fundamental. These self-identities and beliefs serve to define states' perceptions of the situations they face and consequent choices they make in formulating national strategies.[70]

Constructivism's focus on identity and socially constructed spaces makes it particularly appropriate to the cyber realm.[71] The cyber realm is both a physical reality, consisting of computers and networks, and a socially constructed space, where understandings of events and actions depend heavily on how actors choose to interpret events and behave.[72] Any rules or behaviors regarding the cyber realm are, therefore, social constructs, as well, reflecting the self-constructed needs of the actor. States' self-identified needs, culture, and goals, shape the cyber realm into an arena in which they seek to gain a perceived advantage over their adversaries or other actors.[73]

The concept of strategic culture, that is, the milieu in which strategy is considered, debated, and formulated, is closely related to these ideational dimensions of constructivism. Strategic culture is deeply rooted in a nation's historical beliefs, collective memories, values, traditions, mentality, and strategic assumptions.[74] Like culture generally, strategic culture does not determine state choices, but it does have an important impact on the decision-making process that shapes them.

Israel has long perceived its external environment as one of extraordinary and essentially unremitting hostility. The conflict with the Arab states was believed to be existential, long term, and essentially irresolvable. A consequent sense of encirclement and siege mentality, further drawing on millennia of Jewish insecurity culminating in the Holocaust, produced a Hobbesian view of the Middle East and of a generally hostile international order.[75]

In keeping with constructivist arguments, a never-ending quest for ever greater security and emphasis on self-reliance, to ensure national survival, became the core values of Israel's strategic culture. Cultural and strategic beliefs led Israel to view advanced technological capabilities, including cyber, as the basis for the qualitative edge with which it sought to counter Arab quantitative superiority and thus to build the necessary civil cyber ecosystem and military

capabilities. These cultural and strategic predilections were not, however, deterministic and reflected a free and conscious choice, one which then moved Israel down particular paths, while foreclosing other options.[76] For our purposes, the constructivist argument regarding cyber is thus an intervening variable.

If the causal relationship posited in the hypothesis presented here is correct—that strategic and socioeconomic necessity and opportunity, in the face of a particularly harsh external environment, explain the development of Israel's outsized cyber capabilities—a key inference would be that all states would be expected to develop comparable capabilities in response to similar external exigencies. To the extent that this is not the case, and clearly it is not, additional factors specific to Israel must be at play, in this case the intervening variable of strategic culture. Realist arguments explain the basic need that states face to respond to the challenges posed by the cyber realm; constructivist arguments explain why their responses are, nonetheless, widely divergent.

A few words of methodological caution are in order. First, the attempt has been made to present as current a picture as possible of the global cyber threat, the threat to Israel, and the responses it has developed. In a field changing as rapidly and dramatically as the cyber realm, however, this is a Sisyphean effort, and it is almost inevitable that at least some information will be lacking, or already dated, shortly after the book's publication. The manuscript was last updated in the fall of 2021, with some limited additions of importance in spring 2022.

Second, the current state of strategic thinking and capabilities in the military cyber realm has been compared to World War I, in other words, they are still very much in their infancy. As a new threat and realm of warfare, whose ramifications are potentially far-reaching, but still far from understood,[77] it is particularly important that responsible academic study and public discourse take place. This is especially true for a nation like Israel, which faces uniquely severe national security threats reinforced by the complexity of cyber technology that renders it seemingly incomprehensible to the uninitiated and obscures strategic considerations that are frequently quite similar to those from the conventional and more familiar unconventional realms.

Third, for understandable reasons, Israel has said little to date about its military cyber capabilities and strategy, whether in formal policy documents or public statements. Much like other leading cyber powers, Israel presumably fears revealing and thus undermining the advantages it enjoys in this area. An open-source study such as this will, therefore, likely miss some important data and policy considerations. Conversely, there is little doubt that official thinking can be greatly enriched by this study and, indeed, Chapter 12 presents the most comprehensive public proposal to date for an Israeli national cyber strategy, including a first of its kind proposal for a cyber strategy in the military realm.

Lastly, two of the authors are former Israeli defense officials, as a result of which we were required by law to submit the manuscript for a security clearance prior to publication, also a common practice in the United States and other democracies. In any event, Israel is a remarkably open society and readers may rest assured that the clearance process has had little impact on the text before them.

In order to enable the officials interviewed for the book, current and former, to speak freely, they were assured of confidentiality and are usually referred to in the footnotes by an assigned number, rather than name. The interviewees spoke with the clear understanding that they were doing so in their individual capacities and expressing their personal views, not official positions. A list of the interviewees appears in the Appendix.

It is important to stress that the conclusions and recommendations presented in the book are the authors' alone, based on the entirety of the research conducted, and do not reflect official positions, or those of the interviewees. The data presented throughout the book should also not be misconstrued as a confirmation of the events described, merely a summary of the publicly available record.

As a study in political science, the book is designed for four target audiences: First, for cyber practitioners and academic experts around the world, for whom Israel's experience constitutes an important model, because of the lessons that can be applied to their own national needs and the implications for critical policy quandaries, especially given the only limited extant literature on comparative cyber security policies. Second, Israeli practitioners and academics, who may find considerable interest in the detailed accounts, especially the heretofore unprecedented description of Israel's military cyber capabilities, but for whom the book's primary importance may lie in the conclusions and recommendations for policy. Third, for students taking courses on cyber policy, or general national security strategy, for whom Israel's experience provides a unique case of a small regional player with outsized cyber capabilities, approaching those of a global power. Finally, the book is designed to be accessible to a general audience of interested readers, who may not be versed in the cyber realm and whose primary motivation for reading it may be a focus on Israel, but who also wish to gain familiarity with cyber affairs. Other than a few words on terminology in the next chapter, the book does not require technological knowledge to be understood and should be readily understood by all readers.

The book is structured in a manner designed to meet the needs of each of these target audiences, and different readers may wish to read it accordingly, delving deeply into some chapters while skimming or even skipping others. Experts and practitioners in the field may wish to skip sections that are already

familiar to them, while general readers may wish to skim some of the theoretical and background chapters and focus primarily on those dealing with the Israeli experience.

Part I provides the theoretical and practical background necessary to fully appreciate the subsequent discussion of the Israeli experience in Parts II–IV. Chapter 1 provides a general overview of the global cyber threat. On this basis, Chapter 2 then presents the primary cyber attacks that have been conducted, to date, by the leading actors in the global cyber realm; Russia, China, North Korea, and the United States (an entire chapter is devoted separately to Iran, Chapter 5). Chapter 3 presents some of the primary theoretical and policy quandaries of concern both to cyber theorists and practitioners.

Part II presents the cyber threat to Israel. Chapter 4 provides a general overview of the threat and a detailed account of the primary attacks that have taken place to date. Given Iran's importance for Israel, Chapter 5 is devoted solely to its cyber strategy and institutions, as well as the primary attacks it has conducted to date both against Israel and other primary targets. In essence, Chapters 4 and 5 constitute the realist independent variable regarding the strategic imperative behind the development of Israel's cyber capabilities.

Part III presents the Israeli response. It begins, in Chapter 6, with an overview of Israel's strategic culture, including its national security strategy and decision-making processes. The chapter sets out the constructivist argument regarding the intervening variable and provides the background necessary to better understand the different dimensions of Israel's response to the cyber challenge, that is, the dependent variable, presented in the ensuing chapters. Chapter 7 sets out Israel's civil national cyber strategy, as encapsulated in a number of cabinet decisions and a strategic document later formulated by the INCD, including the institutional and legal arrangements. Chapter 8 focuses on one of the most critical components of the civil cyber strategy, Israel's approach to national cyber capacity building, including the remarkable cyber ecosystem it has developed. Chapter 9 addresses another important component of the civil cyber strategy, international cooperation and Israel's approach towards international norms, agreements, and law in the cyber realm. Chapter 10 presents what is publicly known about Israel's military cyber strategy, including the offensive and defensive cyber capabilities it has developed and a breakdown of the defense institutions responsible for different aspects of cyber operations. Chapter 10 concludes with a description of the primary offensive cyber operations purportedly carried out by Israel.

Part IV is the heart of the book and our primary motivation for writing it. Chapter 11 presents the primary conclusions that we were able to draw from both the preceding background chapters and those focusing on the Israeli experience. The conclusions are designed to serve three primary purposes: to provide

at least some answers, based on Israel's experience, to the theoretical and policy quandaries set out in Chapter 2; to present lessons that other states can learn from; and to provide the basis for the recommendations for a comprehensive Israeli national cyber strategy, presented in Chapter 12.

Israel's cyber experience has been truly exceptional, the story of a nation of just 9 million people, no more than a midsized city by international standards, that has become a leader, in both the civil and military realms, in an even more extraordinary global story. There have been missteps along the way, and there are some clouds on Israel's cyber horizons. Nevertheless, the Israeli cyber story has been an overwhelmingly positive and successful one that Israel can be rightly proud of and from which others, both small states and major powers alike, can learn. Importantly, it is a story that is still being written and likely to continue producing striking outcomes in the future.

PART I

MY HOME IS NO LONGER MY CASTLE

The Global Cyber Threat

Part I provides the theoretical and practical background necessary to fully appreciate the subsequent discussion of the Israeli experience in Parts II-IV. Chapter 1 provides a general overview of the global cyber threat. Chapter 2 presents the primary cyber attacks that have been conducted, to date, by the leading actors in the global cyber realm: Russia, China, North Korea, and the United States (Iran is discussed separately in Chapter 5 in Part III). Chapter 3 presents some of the primary theoretical and policy quandaries of concern both to cyber theorists and practitioners.

1

Understanding the Global Cyber Threat

If we end up in a war, a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence.

Joe Biden, President of the United States

We used to say that "my home is my castle," but the information available today about our homes includes the entrance code, combination to the safe and when we plan on being out.

Tamir Pardo, former Head of Mossad

Chapter 1 provides an essential background for readers who are not deeply immersed in the cyber realm and a potentially important refresher for those who are. It is also designed to place the Israeli case in the broader context of the global cyber threat.

Chapter 1 has three sections. It begins with a few simple words on cyber terminology and the common types of cyber attacks (for a detailed description of the different types of attacks see the Appendix). No technological background is necessary, and the text should be readily accessible to all readers. Those readers who are well-versed with the basics of the cyber realm may wish to turn directly to the second section, which provides an overview of the global cyber threat. The third section seeks to identify those characteristics of the cyber realm that are unique, or at least substantially different from existing realms of human endeavor, and those that are not.

A Few Words on Terminology

The rapid pace of technological innovation and ease of information dissemination in today's globalized world provide an ideal medium for the proliferation of a wide variety of cyber attacks. Some forms of cyber attack are fairly simple to

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0002

execute, such as malware easily available on the Internet, and the entry costs are low. All that is required is a computer and some basic knowledge. Attacks such as these can be a nuisance, but do not usually cause substantial long-term harm. At the other end of the scale are highly sophisticated attacks, which are difficult to execute even for state actors but are capable of penetrating well-defended systems. In between are a wide range of attacks, some of which can be used to cause damage to a computer system, or the information in it, or for purposes of espionage.[1]

The terms **cyber realm** and **cyberspace**, typically used interchangeably, refer to the sum total of global computer systems, networks, data, and users. Israel formally defines the cyber realm as "the physical and non-physical area created, or comprised of part, or all, of the following elements: computer systems, computer and communications networks, software, computerized data, content transferred by computer, traffic and control data and the users of all of the above." This definition is relatively standard and is similar to that used by others.[2]

Cyber power refers to a state's ability to use the cyber realm to create advantages over rivals and influence events across the political, economic, military, and other spectrums.[3] **Cyber dependency** refers to the extent to which a state is dependent on computer and communications systems. North Korea, for example, has low cyber dependency and would suffer little damage even from a major cyber attack against it. The United States, conversely, has a very high degree of cyber dependency and is more vulnerable to cyber attack than most other state and nonstate actors.[4]

A **cyber attack** is any premeditated malicious activity designed to disrupt a computer or network, or to collect, disrupt, deny, degrade, take over, or destroy information systems or the information itself.[5] **Malware**, **malicious code**, and **cyber exploits**, frequently used interchangeably, are the means by which cyber attacks are carried out, that is, computer code designed to give the attacker access to a targeted system or damage it. They include **viruses** (malicious code that activates when a file is opened), **worms** (malicious code that spreads without having to open files), **Trojan horses** (malicious code that appears useful but is designed to modify the system or allow remote control of it), and **ransomware** (in which a ransom is demanded as the price of unencrypting a system taken over by the attacker). As early as 2014, 400,000 new types of malware were appearing every day.[6]

Malware is designed to take advantage of **vulnerabilities** in computer systems or software, commonly known as **bugs** or **exploits**. The vulnerability may exist in a well-known application, such as a web browser, or in a subsidiary piece of code. To launch an attack, the attacker must first identify a vulnerability, gain access, and be capable of delivering the malicious code.[7] Attackers will not usually wish to expose the exploits they have developed, because adversaries can patch

the targeted vulnerability and block attempts to use it. An attacker will thus wish to withhold its most advanced exploits until critical moments, but even minor changes to a system can make it harder, even impossible, to penetrate.[8] **Zero day exploits** are previously unknown vulnerabilities, which are of particular use to attackers who wish to maximize their chances of success and minimize the risks of detection. Development of zero day vulnerabilities requires a high level of expertise and is both time consuming and expensive.[9]

Cyber weapons are malicious codes designed to cause physical or functional harm to computer systems and networks. Cyber weapons run the gamut from those that are readily available commercially, easy to deploy, and not highly threatening to sophisticated weapons that require specific target intelligence, considerable investments in R&D, and significant lead time to launch. Low-end cyber exploits can affect the system from the outside but not actually penetrate it, for example, by generating vast traffic that overloads a server or defacing a website. High-end exploits can penetrate even well protected systems and cause direct harm.[10]

Cyber offense and **cyber warfare** refer to the combination of weapons (computer code) and strategies used to design and conduct cyber attacks. The US defines cyber warfare as an armed conflict conducted in whole or in part by cyber means, whether in conjunction with kinetic attacks or independent thereof.[11] Cyber warfare may, or may not, be violent and destructive,[12] although the danger of widespread physical destruction has not yet occurred.[13] It may include such acts as wiping out adversaries' computer systems, halting supply chains, sending military units into ambush, or causing missiles to detonate in the wrong place, satellites to spin out of control, trains to derail, planes to crash, oil to spill, financial systems to collapse, and more. It may also involve psychological and information warfare, or campaigns to sow social and political havoc, such as disrupting elections.[14] **Cyber defense** involves the use of computer code to prevent cyber attacks through a variety of passive and active measures.[15] **Cyber security** refers to a set of policies and actions designed to mitigate security risks and increase resilience.[16]

Hacktivism refers to ideologically motivated cyber attacks designed to draw attention to political, social, or religious causes, rather than to achieve material gain or widespread disruption. Drawing on fluid networks of loosely affiliated activists, pranksters, and hackers around the world, hacktivists are variously described as groups, collectives, movements, or subcultures.

Rapid, superficial attacks typically focus on an adversary's gateway, that is, its website, which is exposed by its very nature both to the public and to hostile actors. The simplest forms of such attacks, **DoS** (denial of service) and **DDoS**, disrupt and deny service, but do not cause substantial or lasting damage. Another common means of attacking an organization's gateway is by automatically

channeling searches to a different site, through attacks on Domain Name System (DNS) servers which are used to route internet traffic. Attacks such as these can also lead to DoS attacks, but are often used for theft of information, reputational damage, exposure to propaganda, or for disseminating information. A common method of damaging a victim's reputation is simply to deface its website.

Advanced Persistent Threats (APTs) are those in which intruders penetrate deeply into computer systems and communications networks and remain undetected for extended periods of time. The technological sophistication required at this level is considerably greater than that required for an attack against a gateway.[17] APTs can attack core operating and operational systems, causing damage to hardware components and either temporary or long-term failures of critical services,[18] such as power, water, communications, and financial and transportation systems, with potentially severe ramifications for large populations.[19]

Another way of differentiating between types of cyber attacks—the one used in this book—is by target and design:

Computer Network Attacks (CNA) seek to disrupt, damage, deny, deface, or even destroy computer systems and networks, that is, cyber sabotage. The damage caused may include temporary stoppage, deletion of data, or paralysis of computer-supported processes. CNA attacks range from easily prevented nuisances to sophisticated attacks with severe consequences. Not being able to access commercial or governmental websites may be inconvenient, but not particularly dangerous. Not being able to access military communications networks may have dire ramifications, as may denial of access to some commercial applications.[20]

Computer Network Exploitation (CNE) attacks refer to the clandestine penetration of computer and communications systems to collect, alter, or delete information for commercial or intelligence purposes, that is, cyber espionage. The data can be technical (about the computers and networks) or informational (such as credit card data, identities of users, or state secrets). CNE attacks can be conducted in preparation for a future disruptive attack (CNA) or for purposes of information operations.[21] While CNE attacks do not cause direct harm and are not an act of war, they can have severe ramifications.[22] To the consternation of innocent computer users, the electromagnetic radiation emitted by key strokes can be used to decipher the substance of the work underway.[23]

Computer Network Influence (CNI) attacks, or cyber information operations, are designed to promote political objectives and even to undermine a government's legitimacy and effectiveness. CNI attacks can include disruption of electoral processes, attacks against political figures and parties, and manipulation of public opinion. They typically make use of social media, **bots** (automated programs designed to mimic humans), **trolls** (professional responders), and fake platforms, all designed to hide the attacker's identity.[24]

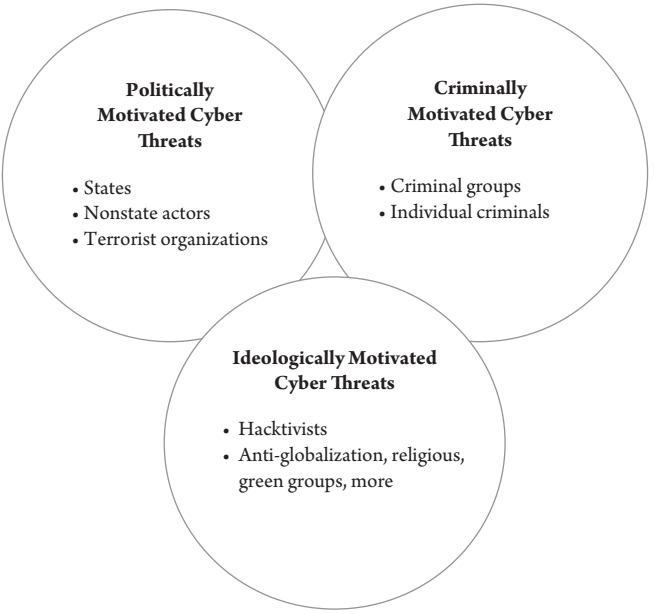


Figure 1.1 Cyber Threats by Motivation

As shown in Figure 1.1, the motivations behind cyber attacks can be divided into three overall categories: **political**, **ideological**, and **criminal**. This book focuses primarily on politically motivated cyber attacks and secondarily on ideologically motivated ones, not cyber crime, but much of what follows is also applicable to it. Politically and ideologically motivated cyber attacks seek to achieve diplomatic, economic, or military advantages over an adversary, or to force it to take unwanted action.[25] They can be launched by states, nonstate actors (such as terrorist groups or nongovernmental organizations), or individuals and may, or may not, cause physical damage. In cases where they do, the physical damage is an indirect, secondary effect, unlike kinetic attacks which inflict direct damage that is the primary intent.[26]

The Global Cyber Threat—An Overview

Cyber attacks threaten the national security of states in a variety of ways: economic, military, political, diplomatic, cultural, and criminal. Cyber attacks are not yet definitively known to have caused fatalities, but they have caused damage to physical facilities, and their capacity to do both appears to be growing. The threat posed by cyber attacks is not only real and growing, but some believe that their growth may even be outpacing the growth of existing national defenses and doctrines.[27]

A sophisticated and determined attacker with adequate resources could cause severe and potentially even devastating systemic damage. Cyber attacks could wreak havoc on civil infrastructure systems essential to day-to-day life, such as electricity, water, communication and transportation systems, leading people to die from cold, dehydration, or car crashes. Cyber attacks could disrupt or take control of monitoring systems at power plants, nuclear reactors, or refineries, causing them to shut down, or far worse. They could derail trains, shut down traffic lights, or take control of autonomous vehicles or commercial airliners in mid-flight. They could access financial networks and modify or erase data, transfer money between accounts, or alter accounts to show zero balances, causing a run on banks and severely disrupting economic activity. Cyber attacks could disrupt emergency response systems, such as the United States' 911 or Israel's 100, or erase or alter population or land registries. They could also disrupt agricultural and food distribution chains, leading to food shortages, as well as manufacturing systems for everything from toys to cars, electronics to vital medicines.

A ransomware attack in 2021 targeted a pipeline operator that carries half of the gas, jet fuel, and diesel used on the US East Coast, setting off panic buying and gas shortages. Had it continued for just three more days, the attack would have shut down mass transit and chemical refineries. Other attacks targeted a major meat packing firm, hospitals, schools, TV stations, basketball and baseball teams, the ferry to Martha's Vineyard, Massachusetts, and more. Raw intelligence about threats that had emerged following the 2021 attack on the US capitol was dumped on the Internet after negotiations with Washington, DC, police broke down over the ransom fee.[28]

Tamir Pardo, former head of Mossad, is an informed and important exponent of the dangers posed by the cyber realm. His alarming vision is worth quoting at length:[29]

> Cyber has become the equivalent of a silent nuclear weapon, the ultimate weapon that can simply take countries apart. Armies were designed to defend national borders, but borders have become meaningless and the battlefield has largely shifted from the military arena to the civilian. A state may be forced to accede to an adversary's demands, or a power station may cease to function, as a result.
>
> Everything is connected to the Internet today and once software can communicate with computer systems, it can also be manipulated. Cellular phone systems can be taken down, or traffic systems disrupted, causing mass paralysis and hysteria. Intellectual property worth billions of dollars can be hacked. University databases can be erased, including students' grades, or even the very fact that they were registered as

students. Medical and insurance systems can be hacked, as can medical devices, such as MRI machines. The manufacturing processes of major corporations can be disrupted.

The world has become completely transparent, providing cyber attackers with almost unlimited possibilities and making everyone subject to potential extortion. We used to say that "my home is my castle," but the information available today about our homes includes the entrance code, combination to the safe and when we plan on being out. People download software onto their smartphones which lets others know everything about them, including their health, finances, love lives and political views. Twenty years ago when you went for a drive, only you knew where you were going. Today, Google Maps means that anyone can know where you are going—and Google even suggests places to shop on the way.

For just a few tens of million dollars, Russian interference in the 2016 US elections undermined faith in American democracy, achieving an effect that no military force could have ever achieved. People no longer have to read a newspaper, or watch TV, to be exposed to information operations, we are all exposed to them through social media almost 24x7. President Trump had tens of millions of followers around the world. Prime Minister Netanyahu could talk directly to the people and no one could dispute what he said, at least in real time. If 3–4 seats in the Knesset were swung by cyber means, the entire political picture in Israel would have changed.

Some fear that cyber attacks could have even more damaging effects than nuclear weapons. As devastating as a nuclear weapon may be, its effects are essentially localized or, in combination, regional. The lethal effects of cyber weapons would be slower, but possibly nation-wide and beyond,[30] what some have called the cyber equivalent of the nuclear realm's mutually assured destruction (MAD).[31] Yigal Unna, former head of the INCD, is one of those who are particularly concerned. "Cyber weapons," he believes, "can be compared to nuclear weapons in their (destructive) power, but the ease with which they can be obtained, or used, makes them more similar to a spear or a bow and arrow."[32] Indeed, cyber attacks on civil infrastructure and other critical capabilities could lead to results that are as debilitating as kinetic attacks, with potentially devastating systemic ramifications.[33] Even if the threat has been over-hyped and most cyber attacks fail, their sheer numbers are such that just a few isolated successes might be sufficient to undermine public confidence in a specific national or international system.[34] In effect, cyber attacks can constitute war by other means.

In the cyber realm, as in other areas of asymmetric conflict, even advanced states do not enjoy a monopoly over the use of force. The very nature of the Internet, its diffuseness and openness, is the source of both the difficulties states encounter in trying to establish a monopoly of force over it and many of the dangers it poses.[35] The Internet was initially developed by DARPA (the Pentagon's Defense Advanced Research Projects Agency) in the 1960s as an informal means of facilitating open communications between scientists, with little thought to considerations of security. The Internet's basic design survives to this day, making it comparatively easy both for state and nonstate actors, even individuals, to take advantage of it for malicious purposes.

Anyone with a computer can now pose a potential threat. Attackers can hack private computers and launch an attack without the owner's knowledge. They can link individual computers to a broader network (known as a botnet or zombie army) originating from a nearly endless number of sources. Moreover, the increasing interdependency of networks means that a successful attack on one has the potential to cause even greater damage by harming all systems connected to it. Whereas a kinetic attack in the past might have been capable of physically destroying a single bank branch, a cyber attack could disrupt or destroy an entire financial network. As more and more global affairs are conducted online in all walks of life, the dangers posed by the cyber realm grow more pressing each day.

The firms that design and manufacture both hardware and software for nearly all electronic devices, including computers, smartphones, medical devices, cars, missiles, aircraft, and more, are dispersed around the world, many in countries with authoritarian governments. Any one of these firms could install hidden code in devices for espionage or destructive purposes. The United States was deeply concerned that 700 million smartphones made by Huawei and ZTE, for example, two of China's largest manufacturers, had software implanted in them that would enable the Chinese military to spy on users' movements and communications.[36]

Cyber capabilities are increasingly prevalent and easily accessible. Hackers, whether individually, or as parts of groups, sell capabilities online, and the decentralized nature of the Internet makes it easy for a black market of malicious services, technology, and expertise to flourish.[37] While not always cheap, the tools and expertise required to gain access to a network, conduct automated searches for vulnerabilities, and deliver a wide range of payloads are not prohibitively expensive. Small scale cyber capabilities truly are inexpensive and even sophisticated ones, which make use of rare vulnerabilities, are available for purchase. In the past, hackers typically sought to sell newly found zero day vulnerabilities back to the original software vendor, but as their price has risen, they are increasingly selling them to state and nonstate actors as well.[38] The markets themselves are growing increasingly sophisticated.[39] One company has

a database showing the physical location and Internet addresses of hundreds of millions of vulnerable computers around the world and has identified target packages in Russia, China, the Middle East, and Latin America. It also sells zero day exploits to governments, including the CIA, US Cyber Command, and British intelligence, as well as to major corporations.[40]

Cyber black markets also provide a venue for intelligence collection. Information stolen from governments and private entities is available for purchase and can enhance a potential attacker's chances of success.[41] On-line forums provide nonstate actors with an opportunity to discuss and test their payload designs and could help a well-funded and determined nonstate actor develop the truly sophisticated capabilities that are usually limited to state actors.[42]

Some of the capabilities available are sophisticated enough to penetrate even comparatively well protected computer systems, including those of governmental networks, defense contractors, communications providers, and commercial firms. The good news is that there is only limited evidence, to date, of nonstate actors having successfully penetrated highly secure governmental networks.[43] The bad news is that this is not true of state actors and that the tools already available, including advanced cyber exploits stolen from state actors such as the US National Security Agency (NSA), can provide most nonstate actors with a massive boost to their capabilities and cause disruptions to daily life. As they improve, it is increasingly likely that nonstate actors will be able to breach sensitive governmental systems as well.[44]

States' growing dependence on the cyber realm has opened up vast new opportunities to cause harm, both by other states and nonstate actors, including terrorist organizations, providing them with the potential to achieve previously unimaginable damage and effects. The cyber realm is particularly attractive for nonstate actors, for a number of reasons. Cyber attacks remain inexpensive compared to kinetic means, and the cyber realm provides an unusual degree of anonymity and freedom to strike adversaries behind a veil of plausible deniability. Moreover, to be an effective actor in the cyber realm, it is not necessary to have control over territory or infrastructure, two critical advantages for nonstate actors.[45]

Nonstate actors have little trouble attacking less well defended targets and may prefer them, at least when the objective is merely to disable or slow systems, deface websites, or conduct espionage and theft of information. Attacks such as these do not generally cause great damage, although complex systems and websites that do not work can have significant economic costs or complicate communications between a government and its public in emergencies. "Death by a thousand cuts," or constant low-level attacks against commercial and governmental networks, is one way that nonstate actors may seek to slowly undermine a state's economic system and public morale and potentially force it to make concessions.[46]

Conversely, most nonstate actors do not have the capabilities necessary to hit the most valuable and usually best defended targets. To succeed, attackers must be capable of developing unique capabilities tailored to the specific target system and usually have to test them in advance to make sure that they work. Doing so takes time and requires significant resources, including a substantial investment in R&D and intelligence on the system in question. It also usually requires the ability to put together multiple complex teams with different professional skill sets.[47]

The British government assesses the cyber capabilities of terrorist organizations as low and predicts that their primary focus for the foreseeable future will remain on kinetic attacks, rather than cyber terrorism. Nevertheless, it maintains that even the limited cyber capabilities available to them have had a disproportionate impact, as simple defacements, or hackings of personal details, have garnered considerable media attention and intimidated their victims—the very essence of terrorism. Even more worryingly, a generation of increasingly computer-literate terrorists will likely succeed in conducting more disruptive attacks, with the potential for a limited number of advanced ones.[48]

There have yet to be cases of cyber terrorism that caused direct physical effects, despite the expressed desire of various terrorist organizations, such as al-Qaeda and the Islamic State, to do so.[49] Terrorist organizations have made extensive use of the cyber realm, to date, for purposes of operational planning, recruitment, training, fundraising, communications, espionage, propaganda, and information dissemination operations designed to sow fear and dissension. Moving forward, the obstacles to physical cyber terrorism could be overcome if state actors with advanced cyber capabilities were willing to provide them with the necessary assistance, as Iran is suspected of doing with Hamas and Hezbollah.[50]

Some of the attributes of cyber attacks that make them attractive for nonstate actors, such as their relative deniability, low cost compared to conventional military capabilities, and ability to conduct information operations with potentially far-reaching ramifications make them similarly attractive for state actors. This is true today both of global powers, such as Russia and China, and rogue states such as Iran and North Korea.

Western states have grown increasingly alarmed over the dangers posed by malign information operations. In response, the UK, for example, established a National Security Communications Unit within the Cabinet Office, designed to conduct "rapid responses" to disinformation campaigns by state and other actors.[51] France set up an agency, under its equivalent of the US National Security Council (NSC), to combat foreign disinformation and fake news by identifying cyber information attacks "from a foreign country or organization that seeks to destabilize the state politically." The new agency was not to be another intelligence service, nor was it to address the actual veracity of the information

disseminated, and its activities were to be vetted by an ethics committee drawn from the judiciary, diplomatic corps, media, and research communities. In the United States, the State Department established a Global Engagement Center tasked with identifying and countering foreign propaganda and disinformation,[52] the director of national intelligence set up a Foreign Malign Influence Center to track abuse of social media by state and nonstate actors, and the Department of Homeland Security has convened an internal working group to address the issue.[53]

What Is Different about Cyber—and What Is Not

Cyber is an exciting new realm of human endeavor that has caught the imagination of many. It is, however, still only partially understood by most, and even experts hotly debate its theoretical attributes and strategic ramifications. The following section seeks to characterize those attributes of the *cyber realm* and of *cyber attacks*, specifically, that are unique, or at least substantively different from long-existing domains and types of warfare. The section thereafter then turns to areas of continuity and that which is not different about cyber.

What Is Different about the Cyber Realm

An Entirely Human Creation and a Substrate: Not Just Another Realm—unlike the long-existing domains of military operations (land, sea, air, and space) and most other areas of human endeavor, the cyber realm is an entirely human creation and under the control of human architects.[54] Moreover, the cyber realm is not just a new domain, but a substrate, an underlying layer that is crucial to every facet of modern life: political, social, economic, cultural and military.[55]

Unprecedented Proliferation of Disruptive Technologies—railways, the telegraph, radio, aircraft, and the atom, among others, were all disruptive technologies in their day that dramatically changed civil and commercial life and rapidly gained military applications. The impact of cyber technologies, however, on all walks of life, is unprecedented, both in pace and scale. No other technology has produced such disruptive and even revolutionary applications on a global scale, both civil and military.[56] Waze and Uber revolutionized transportation, Amazon retailing, Google access to information, Skype communications, Facebook social life, Airbnb recreation, Zoom work, and digitization generally how we organize militaries and wage wars. The list goes on—and the changes have just begun.

Challenges to the Concept of Statehood—states do not enjoy a monopoly over force in the cyber realm, traditionally a fundamental attribute of statehood, and

certainly have less control over their cyber borders than physical ones. Most cyber attacks take place against individuals and public and private organizations, not states, and given the vast numbers of attacks, only they can bear ultimate responsibility for their defense, not their governments.[57] As demonstrated by such diverse political events as the "Arab Spring" and attacks against Ukrainian and US elections, the cyber realm also provides unprecedented opportunities to mobilize or disrupt political processes and even undermine governments. Google and other tech giants have more information, digital power, and cyber capabilities than many states and control a global cyber infrastructure that rivals the importance of states' national infrastructures.[58]

Changes to the Nature of Warfare—the old metrics of military power are no longer fully applicable and even misleading. Unlike traditional warfare, cyber power is not primarily about the size and quality of a state's armed forces. Cyber attacks are much cheaper than conventional or unconventional ones and can be carried out by comparatively small numbers of people, without the need to maintain entire armies or conquer and occupy territory. They may, however, enable a previously unattainable degree of systemic disruption, including the ability to do so without physical devastation. Many of the most important targets in the cyber realm are not military, but civil or commercial. Organizations, or more specifically organizational information systems, are often the new battlefields and as such must be the focus of any cyber security strategy. Private firms provide both offensive and defensive services in the cyber realm to an extent that does not exist in the physical world, proliferating advanced capabilities to governments that are unable to develop them on their own and augmenting the capabilities of leading state actors that are.[59]

What Is Different about Cyber Attacks

Immediacy—cyber attacks happen instantaneously, with the stroke of a key on a computer, making it difficult to prepare defenses and denying decision-makers the time needed for a considered response. Indeed, in the short term, only pre-planned automated responses are often possible.[60] Surprise attacks are simpler as well, because attackers do not have to assemble and move equipment, weapons, and military formations. Conversely, it is difficult to modify code once developed for a given target system and not all stages of cyber attacks take place at machine speed; the planning and preparation of a sophisticated cyber attack are done at human speed, over months or years.[61] Even then, however, activation is instantaneous.

Super Empowerment—kinetic attacks require state-based capabilities, or at least those of a terrorist organization, while anyone with a PC can cause at least some degree of harm. The "big data" capabilities that were once the sole province

of governments and major corporations are now available to anyone at minimal or no cost, including the ability to collect, evaluate, and analyze vast quantities of information.[62] Sophisticated cyber attacks require technological capabilities that exceed those of an individual, though maybe not those of a well-funded nonstate actor, and may achieve unprecedented affects. ISIS and other terrorist organizations have put cyber capabilities to extensive and effective use. Small states can develop outsized military cyber capabilities. Eight decades after the advent of nuclear weapons, only nine countries are thought to possess them; dozens of states have offensive and defensive cyber capabilities.[63] Advanced states are achieving heretofore unimaginable effects in cyber intelligence and information operations.

No Geographic Limits; Global Reach—unlike all other weapons systems, conventional or unconventional, cyber weapons have no geographic limitations and ignore national borders. They can be launched concomitantly around the globe, against a virtually unlimited number of targets, in some cases crossing borders without states even knowing that their networks have been used and their sovereignty violated. In so doing, they essentially neutralize both time and space.[64]

Systemic Disruption and Even Destruction—cyber attacks have the potential to cause disruption on a heretofore unprecedented systemic scale. Whereas the effects of all other weapons are localized, even nuclear weapons, those of cyber attacks can be nationwide, even global, severely degrading an adversary's economy or military capabilities. A conventional or terrorist attack in the past could have destroyed a bank, hospital, or private property, a cyber attack could wipe out an entire financial or health system, or cause chaos by erasing a national land or population registry. Disruption of enemy radar, or command-and-control system, could blind it to an attack or render it incapable of responding. A nationwide, or even regional, disruption of an adversary's electric grid could cause social and economic havoc[65] and determine the outcome of a military confrontation.

Lethal and Non-Lethal Uses—kinetic weapons are intentionally designed to cause physical damage and even loss of life. Cyber weapons usually do not have lethal effect, although they can cause severe harm and even damage a state's ability to function. Military operations that would have necessitated a loss of life in the past, on both sides, can be achieved with few casualties. if any, by cyber means. Espionage can be conducted through computer intrusions, without endangering the lives of spies.[66]

Pinpointed Attacks; Minimal Collateral Damage—cyber weapons can be targeted against specific sites with a degree of precision that is hard to achieve with kinetic attacks, including distant facilities with strong physical defenses or embedded among civilians, thereby minimizing collateral damage. Moreover, the effects of cyber weapons can be intentionally temporary and even reversible.[67]

Attribution Is More Difficult—when a state or nonstate actor launches a kinetic attack, it is fairly easy to determine that it has taken place and attribution is usually straightforward (less so with chemical and biological weapons). In the cyber realm, attackers can more easily disguise attacks and cause damage without leaving evidence. The target may not even know that it has been attacked. Assigning attribution for cyber attacks is thus more difficult than in the physical realm.[68]

Cyber Weapons Are Not Fungible—the computer code developed for cyber weapons, especially sophisticated ones, is target-specific. Code developed to attack a surface-to-air missile system, for example, may be of no use against another system of this type, or an air-to-air system, and even minor changes to the targeted system can render the offensive code useless. In contrast, essentially all conventional and unconventional weapons can be used against a variety of targets, with some time for adjustments.[69]

Unclassified Information of Top-Secret Importance—intelligence agencies were forced to go to great lengths and risks in the past to gain classified information, in some cases even unclassified. Cyber intelligence, using big data systems, can put together enormous quantities of unclassified information, each piece of which is of little importance in and of itself but which together provide a picture that is at least as rich as that which can be gained through costly and dangerous covert means.

What Is Not Different about Cyber Attacks

The previous section's contentions notwithstanding, some scholars question whether the cyber realm really is all that different from the physical one and whether the threat is all that new. Warfare is constantly changing, but the cyber realm, they maintain, does not fundamentally change military or foreign affairs, and the dangers are overstated.[70]

Meaningful Damage and Policy Change Are Hard to Cause through Cyber—critical systems are generally well defended, many are not connected to the Internet, and the impact of cyber attacks tends to be temporary and reversible. Whether cyber attacks truly have the capacity to cause significant damage to technologically advanced states in the cyber realm is a subject of debate. Moreover, in the absence of physical damage, cyber attacks alone are not likely to force changes in states' policies and will usually only prove useful as part of a broader effort that also includes kinetic operations and other instruments of policy.[71]

Cyber Is Similar to Long-Standing Asymmetric Threats—the threats posed by the cyber realm share numerous characteristics with asymmetric threats in the physical world. Terrorist threats, like cyber ones, have become global, with major terrorist organizations operating around the world and leaving defenders in both areas with an enormous number of targets to protect, including civilian ones. For a variety of reasons, including their ability to blend into civilian populations, it is extremely difficult to truly defeat either terrorist organizations or malicious cyber actors. Decisive victory is hard to achieve in either area, but strategies that have been applied for purposes of counter terrorism, including gradual and cumulative approaches, are also likely to be applicable to the cyber realm.[72]

Cyber Capabilities Are Difficult and Expensive, If You Want Them to Work—creating effective cyber weapons and defenses requires highly developed technical capabilities, advanced R&D teams, the ability to test the weapons developed, and more. Actors also need effective intelligence capabilities to gain highly detailed information about the target, in order to ensure that a cyber weapon actually works, as well as effective command and control systems and well formulated cyber policies and strategies. The cost of doing all of this is not inexpensive and takes time, so cyber operations are best suited to actors with long-term foreign policy and military strategies and substantial resources.[73] It is cheap, however, compared to conventional and unconventional weapons and warfare.

*Super Empowerment, but for Advanced Actors—w*hile anyone with a computer can launch a simple cyber attack, the resources and knowhow needed to successfully conduct sophisticated attacks are beyond the capabilities of all but a handful of advanced nonstate actors and even the vast majority of states. As such, cyber does not actually empower weaker actors, but instead may further widen the gap between stronger and weaker actors in favor of the former. Cyber does provide new means of conducting espionage, causing damage, and manipulating information, but does not meaningfully change the power structure of the international system.[74]

Cyberspace Is Not a Lawless Wild West—cyber does pose new problems of attribution, but this is not fundamentally different from chemical and biological weapons. Moreover, both cyber security firms and state actors have constantly improved their forensic and intelligence tools and attribution is not an insurmountable obstacle. There is also little evidence to substantiate fears that cyber will prove to be dangerously escalatory. With few exceptions, states have responded to cyber attacks symmetrically, with cyber attacks of their own, and proportionally, in a manner designed to reduce the dangers

of escalation. Although an accepted body of international cyber norms and law have yet to emerge, there is a growing consensus that international law is applicable to the cyber realm and that cyber attacks can violate international prohibitions on the use of force and trigger states' customary right to self-defense.[75]

Challenges to the Concept of Statehood Are Not New—new technologies have long posed challenges to existing concepts of statehood, even to regime survival. The emergence of the sea, air, and space as economic and military domains posed unique challenges to the traditional concepts of statehood of their time, upending accepted modes of commerce, diplomacy, and warfare and providing states with new means with which to gain international influence. The cyber realm certainly provides new means of conducting political discourse and information operations, but does not fundamentally change them. The Iranian revolution in 1979 was conducted with the aid of cassette tapes, the technology of the day. Just as with new technologies of the past, states can and already are developing ways to protect themselves. They may, in fact, be able to create a "cybered Westphalian age," in which states erect virtual fences to control the flow of information within their national cyber realms and protect their sovereignty.[76]

A Weapon Is a Weapon—cyber weapons differ in some obvious ways from kinetic weapons, but are not fundamentally different in nature. Much as a bullet, once fired, is useless and new ones must be manufactured, so too, cyber weapons may be short-lived and even single use. Claims that cyber weapons are "use or lose" are questionable. Just as the inability to predict when an adversary will make changes to a system or patch a vulnerability generates incentives to use a cyber weapon before the opportunity is lost, mobile kinetic weapons can be moved and hidden. Although the immediacy of attacks is unique to the cyber realm, the development of sophisticated weapons can take years and defenders in the physical realm often do not have much time to respond to attacks either. Moreover, the immediacy of kinetic military capabilities is also increasing and both kinetic and cyber weapons can be proliferated.[77]

Similar Strategies and Organizations Provide the Response—given the many similarities between the cyber and physical realms, the agencies responsible for formulating and implementing policy in both are similar in nature. The United States, for instance, established a Cyber Command that is organized like a traditional military command, and its military cyber strategy borrows greatly from existing concepts of conflict and warfare.[78] The same is true of other state's cyber strategies, and even where differences do exist, the core ideas remain the same.

These are important arguments, and we take them all seriously. Certainly, not everything about cyber is truly and fully new. Nevertheless, not everything

about a new realm must be substantively different from long-existing realms and threats for it to warrant special attention. Even small differences, and in this case they are not small, can make a critical difference. In the debate between those who believe that cyber does present a substantially new realm and those who believe that it does not, we lean toward the former.

2

Primary Cyber Attacks around the World

[The US faces] a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life that would paralyze and shock the nation and create a profound new sense of vulnerability.

Leon Panetta, US Secretary of Defense

There are two kinds of big companies in the United States. There are those who have been hacked by the Chinese and those who do not know they have been hacked by the Chinese.

James Comey, FBI Director

Chapter 2 surveys the primary cyber attacks that have taken place around the world to date, both as basic background for readers who may only have limited familiarity with the cyber realm and to further place the cyber threat to Israel in a broader perspective. The number of such attacks is vast and could fill an entire tome in their own right. The chapter thus focuses on those conducted by just four of the leading global cyber actors—Russia, China, North Korea, and the United States—against both state and nonstate actors around the world. Attacks by these actors against Israel are presented in Chapter 4. Attacks conducted by Iran, against Israel and international actors, are presented separately in Chapter 5.

As a quick reminder (see Chapter 1 for greater detail), Computer Network Attacks (CNA) seek to disrupt, damage, deny, deface, or even destroy computer systems and networks, that is, cyber sabotage. Computer Network Exploitation (CNE) attacks refer to clandestine penetration of computer and communications systems to collect, alter, or delete information, for commercial or intelligence purposes, that is, cyber espionage. Computer Network Influence (CNI) attacks, or cyber information operations, are designed to promote political objectives and even to undermine a government's legitimacy and effectiveness. CNI attacks can include disruption of electoral processes, attacks against political figures and parties, and manipulation of public opinion.

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0003

Russian Cyber Attacks

CNA attacks—in 2007 Russia was reportedly behind a three-week wave of cyber attacks against Estonia. The attacks, the first known incidence of a widespread and coordinated cyber campaign perpetrated by one state actor against another, was subsequently dubbed—not without some hyperbole—Web War 1.[1] Estonia, at the time, was one of the world's most connected nations and was thus particularly vulnerable to the Russian campaign. DDoS attacks disabled the websites of government ministries, political parties, and various firms; ATM's and online banking services shutdown sporadically; government employees were unable to communicate by email; and newspapers and broadcasters could not deliver the news. The Russian attacks were not armed attacks in the traditional sense, since they did not involve physical force, or aim to cause destruction or death, but they were clearly designed to achieve political aims through coercion. Considerable evidence existed that the Russian government was behind the attacks and Estonia, a NATO member, turned to the alliance for support. The proof, however, was not conclusive and the lasting impact on Estonia's infrastructure and economy was minimal. In these circumstances, none of the other NATO members deemed a military response, or even a strong non-military one, to be warranted.[2] Estonia was left to fend for itself.

In 2008 a conflict broke out between Russia and Georgia for control of South Ossetia. Unlike the Estonian case, this time Russia combined infantry, armored, and air attacks with cyber attacks against Georgian governmental websites, servers, and media outlets. The attacks did not cause physical damage, but they did undermine the efficacy of the Georgian government at a time of crisis and hinder its ability to communicate internally, coordinate an effective response and inform the world of its side of the conflict. As in Estonia, the evidence directly linking the Russian government to the attacks was considerable, but not incontrovertible.[3]

Ever since 2014, Russia has repeatedly targeted Ukraine with cyber attacks in order to undermine its independence and growing relationship with the West and NATO. Virtually every sector of Ukrainian life has been attacked in the attempt to exacerbate the nation's political divisions, degrade its state institutions, and undermine public confidence in everything from elections to the judicial system and government. On election day in 2014, pro-Russian hackers (with links to those who later attacked the Democratic Party during the 2016 US elections) hacked the website of the Ukrainian Central Election Commission and altered the real-time voting results it was providing to television networks. The hackers presumably knew that the fake results—which showed that the Kremlin's preferred candidate had won—would be exposed quickly but simply

sought to create chaos and undermine the legitimacy of Ukraine's political system.[4]

Attacks against Ukraine's power grid in December 2015 and 2016, attributed to Russia, left hundreds of thousands of people without electricity for hours, in the dead of winter, but may have actually been designed to cause lasting physical damage. In 2017, at the height of the tourist season, two of Ukraine's international airports were hit by cyber attacks, as were the ticketing system in Kiev's subway, supermarket checkouts, bank ATMs, and the radiation monitoring system at Chernobyl,[5] the site of the world's worst nuclear disaster to date.

Later in 2017, Russia is believed to have been responsible for the most costly and destructive cyber attack ever conducted, the NotPetya attack against the Ukrainian government, banking system, and power grid. Altogether 300 Ukrainian companies were targeted; 30% of the nation's computers were paralyzed and 10% erased completely, including those used for the Chernobyl cleanup. Frantic attempts by operators at power stations to bring them back online proved futile and possible backup sources of power were also intentionally disabled. NotPetya exploited vulnerabilities common to the operating systems of numerous applications and thus spread rapidly to 64 countries, including the United States, Poland, Germany, Italy, and even Russia itself. A whopping 200,000 computers were affected, causing $10 billion in damage to FedEx, Merck pharmaceuticals, Maersk shipping lines, and others.

The Russian campaign in Crimea went even further, molding cyber and conventional operations into a unified strategy of hybrid warfare, known as the Gerasimov Doctrine, after Russia's chief of staff. The basic model, which combines conventional attacks, terrorism, economic coercion, political maneuvering, and information operations was not new. Russia had applied it often in the past, but the speed with which social media facilitates the spread of information and its low costs greatly amplified the campaign's effectiveness.[6] For Russia, information operations are means of achieving strategic objectives, including the destabilization of target states, without the need to resort to kinetic conflict.[7]

The campaign in Crimea further reaffirmed the validity of one of Gerasimov's fundamental tenets; as long as a hybrid attack remained ambiguous in nature, deniable, and drew only limited bloodshed, the United States and other countries would be hard pressed to mount an effective response. Some believe that Russia has used Ukraine as a real-world testing ground to demonstrate its ability to conduct cyber campaigns against the United States and deter it from infringing on Russian interests. Whatever the motivation, Russia had sent the United States a powerful signal: it could undermine a foreign opponent.[8]

In 2022, as Russia built a massive force on Ukraine's borders in preparation for a possible ground invasion, 70 Ukrainian government sites were disrupted.

In a public message the hackers warned "Ukrainians! All of your personal data was uploaded to the Internet. All data on the computer is being destroyed. All information about you became public. Be afraid and expect the worst."[9]

Between 2015 and 2017, Russian cyber attacks penetrated the computer networks of US and European nuclear power reactors, electric grids, industrial systems, and communications networks. In 2017 they had reached far enough into a US power plant to manipulate its controls, stopping just short of sabotage. That same year hackers, apparently Russian, took control of an emergency shutdown system designed to prevent catastrophic explosions at a Saudi petrochemical plant. The attack is believed to have been the first case of malware explicitly designed to trigger an explosion that was likely to cause fatalities, not just destroy data or shut down an industrial operation. Thousands of industrial plants around the world rely on the same computer systems. Fortunately, an error in the computer code led to the attack's failure.[10]

In 2018 Russia sought to disrupt the Winter Olympics in South Korea, in retaliation for its humiliating ban from the prestigious competition due to violations of anti-doping rules. Russian hackers, impersonating officials of the International Olympic Committee (IOC) and the Korean government, gained access to the Olympics digital infrastructure by sending malware-laden emails to members of the IOC, athletes, and companies. Once inside, they were able to disrupt Internet access, telecasts, and Olympics websites and prevent spectators from attending the opening ceremony. The Russian hackers apparently also sought to disrupt the Tokyo Olympics originally scheduled for 2020, using North Korean tools to hide their tracks.[11]

By 2018 the United States and UK had come to suspect that Russia had targeted millions of devices in both countries, including routers in private homes and small businesses and the increasingly widespread IoT, apparently as a prelude to future attacks against critical infrastructure, governmental computer systems, and more. Indeed, they grew so concerned that the two governments issued a highly unusual joint warning in the attempt to deter Russia from further attacks.[12]

CNE attacks—in 2008 Russia conducted the first successful cyber attack against a classified, air-gapped, US military communications network, which connected top military commanders to senior officials in the White House and intelligence agencies. The technique used was shockingly simple. The Russians scattered USB drives around a US military base, someone picked one up, connected it to a laptop and the Russians were in, with access to the entire US network. The attack was discovered early, and little damage was actually done, but the potential ramifications were severe.[13]

Russia's audacious cyber information campaign against the US elections in 2016 may have been emboldened by its successes the previous year, when

Russian affiliated hackers, operating around the world to hide their tracks, conducted a sophisticated penetration of unclassified, yet still sensitive, computer systems at the White House and State Department.[14] Later in 2016 some of the NSA's most advanced and sensitive cyber exploits—the actual codes it had used to place implants in Russia, China, Iran, and other targets—began appearing on the Internet. A group of Russian hackers, known as the Shadow Brokers, posted the codes for all to see and use, even offering an entire product catalog.[15]

In 2020 the APT29 hacking group, aka CozyBear, the same Russian hackers who had compromised the Democratic National Committee and penetrated White House and State Department email systems, attacked again. This time they targeted a variety of US, British, and Canadian health organizations involved in the development of the coronavirus vaccine, including pharmaceutical firms, hospitals, research laboratories, healthcare providers, and the US Department of Health and Human Services. The attack included both spearfishing and malware and was designed to steal information in order to accelerate development of the Russian vaccine, but not, apparently, to sabotage the targets' development programs.[16]

While the vaccine-related attack was underway, one of the worst cyber attacks in history, a Russian cyber espionage campaign of global proportions, came to light. It began with an attack on FireEye, one of the premier providers of cyber security services to governments and companies around the world and was apparently also perpetrated by APT29/CozyBear. In this case, the hackers stole FireEye's "red team tools," highly sophisticated hacking capabilities that it used to test its clients' computer systems for vulnerabilities. The hackers went to extraordinary lengths to hide their tracks, creating thousands of new Internet protocol addresses in the process, many inside the United States. The *New York Times*, marveling at the audacity of the attack, likened it to bank robbers stealing the very tools that the FBI was using to investigate the robbery they had committed.[17]

The Russian cyber espionage campaign, which may have actually begun a few years earlier, reached a critical turning point when malware was inserted into an automatic software update in Orion, a network management tool made by a firm called SolarWinds. Once inside Orion, the attackers were able to make use of the fake identification tokens used by Microsoft, Google, and others, to verify the identity of computer systems, roam freely around them until discovered nine months later, and gain access to the sensitive parts of the networks, including data stored on in-house servers and cloud data centers. Had they chosen to do so, the attackers could have conducted highly destructive attacks, changed data, or taken control of industrial processes. They also gained access to Microsoft's

source code, thereby enabling them to search for software flaws that might be exploited for future cyber weapons.[18]

Approximately 33,000 SolarWinds customers around the world used the Orion software, including 425 of the Fortune 500 companies, of whom some 18,000 downloaded the Russian malware. The hackers have truly exploited tens of high-value networks, mostly in the United States but also in seven other countries: Canada, Mexico, the UK, Belgium, Spain, the UAE—and Israel.*

The attack on SolarWinds was first detected by FireEye, not the US government. In practice, the Russian hackers had specifically designed the attack to avoid alerting the sensors that the United States had placed both on domestic and foreign networks, using US Internet addresses and, most importantly, targeting a peripheral administrative system like Orion. To further elude US defenses, they also took advantage of legal prohibitions that prevent the NSA and CIA from conducting surveillance of domestic networks. Even more worryingly, the hackers made use of multiple entry points, in addition to the Orion update, and additional supply chain vendors, thereby indicating that the attack may have been even more widespread than known.

The SolarWinds attack was limited to espionage; no systems were damaged or disrupted. Nevertheless, the scope of the attack and potential for damage were staggering. Whereas intelligence agencies in the past had to go to great lengths to gain access to just a single target, the SolarWinds attack was able to breach the technology supply chain of thousands of government agencies and firms around the world. Moreover, SolarWinds is just one of hundreds of relatively unknown companies that provide network software to governments and businesses, and which are themselves dependent on numerous other software and hardware manufacturers. Months after the attack, following a review of US cyber security policy, President Biden explained that he had chosen to respond "proportionally" to the Solar Winds attack because he did not want "to kick off a cycle of escalation and conflict with Russia."[19]

* High value targets, from whom information was potentially stolen, or altered, include the US Departments of State, Defense, Treasury, Commerce, and Justice, NSA, National Nuclear Security Administration (which maintains the US nuclear stockpile), Sandia and Los Alamos national nuclear laboratories, NASA, Center for Disease Control, state and local governments, AT&T, Visa, Lockheed Martin, Ernst & Young, the *New York Times*, and critical infrastructure and technology firms such as Microsoft, Intel, Yahoo, and Cisco. A number of Original Equipment Manufacturers (OEMs), which provide services to critical infrastructure firms, were also infected and in turn infected some of their customers. Making matters worse, some OEMs have access to customers' networks, so that they can make necessary changes, install new software, and conduct critical operations, meaning that the hackers could have gained control, for example, over turbines for power generation and access to thousands of more systems.

Just months after the SolarWinds attack, the same Russian hackers attacked 3,000 email accounts and 150 government agencies and think tanks in 24 countries, though mostly in the United States, apparently in the attempt to infiltrate groups that had, among other things, revealed Russian disinformation campaigns. They also targeted over 140 technology companies, possibly indicating that the campaign was designed to gain long-term, systematic access to various points in the technology supply chain.[20]

CNI attacks—the Russian information operation during the 2016 US presidential elections was probably the most prominent cyber campaign ever conducted. The initial intent was apparently to use attacks on the email servers of the Democratic National Committee and Clinton campaign to embarrass Clinton and hurt her chances of election. Once Clinton became the front runner, however, the Russians' shifted to a social media campaign designed to sway the outcome in favor of Donald Trump, or at least undermine Clinton's stature as a future president. Russia may have believed that a Trump victory would undermine Western confidence in US leadership and help bring about its decades-old strategic objective of weakening NATO,[21] an objective that was at least partially achieved.

By exposing the vulnerabilities of the US electoral system and further aggravating socially divisive issues, the Russian campaign may even have been designed to erode popular faith in the basic legitimacy and efficacy of US democracy. To this end, the Russians targeted specific groups of voters in swing states, including African Americans, Latinos, gays, environmentalists, evangelicals, and veterans, with tailored messages on controversial issues, such as gun control, minority rights, and immigration. A self-styled Heart of Texas group was ostensibly based in Houston but actually operated out of Moscow, while another group Stop Islamization of Texas was opposed by United Muslims of America. In both cases, rallies were organized by real groups of Americans who had joined Facebook pages set up by the Russians. Fear and discord were further sown by text messages that warned of toxic fume released from a chemical plant in Louisiana—which did not exist—and by rumors that the Ebola virus was running wild in parts of the United States.

The Obama administration even feared a Russian attempt to sabotage the elections themselves, for example, by changing Social Security numbers, deleting voters from the rolls, or plunging key cities into darkness. The administration publicly accused Russia of interfering in the elections, the first time the United States had ever accused a foreign state of a significant attempt to do so, and considered a range of possible responses, some extreme, such as cutting Russia off from the international banking system. In the end, however, it decided to respond with restraint, largely out of fear of appearing partisan or of playing into Russia's hands by publicly conceding that the elections had been compromised and the US democratic system subverted.[22]

The scope and actual effectiveness of the Russian campaign in the 2016 elections were the subject of an inquiry by a special investigator and are still subject to debate, but the very fact that it took place illustrates the increasing dangers and myriad malign ways that the cyber realm can be abused. At the very least, it succeeded in placing the administration in a lose-lose situation, and the damage to public confidence in the integrity of the electoral process was a major success.

Subsequent Russian cyber attacks on the 2017 French presidential elections, though successfully blocked, and reports of possible attacks on the German and Dutch elections and on public referendums that year in Britain, Holland, Italy, and Spain, created a sense that the West as a whole was being targeted. In all, US and other Western intelligence agencies estimated that Russia conducted information campaigns against 19 different countries in an effort to weaken NATO and split the Western camp, promote separatist-nationalist agendas, exacerbate social cleavages, and, above all, undermine public faith in Western democracy and institutions. In 2021 Germany accused Russia of interfering in its elections that year.[23]

Russia apparently tried to interfere once again in the US 2018 midterm and 2020 presidential elections. In the latter case, Russian intelligence agencies conducted a disinformation operation designed to sow divisiveness and discord and to disrupt the elections. This was to be achieved both by casting doubt on the legitimacy of the electoral system and by denigrating former Vice President Biden, in the hopes that Russia's preferred candidate, President Trump, would prevail. Russian interference began with support for Senator Bernie Sanders during the Democratic primaries but then transitioned to two mutually supporting approaches. On one level, they amplified misleading statements made by Trump himself, especially about the dangers of mail-in ballots. On the other, they prepared ransomware attacks against state and local electoral systems which would have made it difficult to count votes or certify tallies, had they remained undetected. In so doing, the Russians sought to cast doubt on the outcome of the elections and feed into the narrative that Trump himself was promoting regarding the validity of a possible Biden win.[24]

Chinese Cyber Attacks

China is one of the more advanced and aggressive actors in the cyber realm and its cyber warriors are thought to number in the tens of thousands.[25] For China, the cyber realm poses both a potentially significant threat to its domestic stability and regime legitimacy, but it is also a way of countering comparative US strength and an engine of economic growth. Some believe that China even views the cyber realm as a means of achieving a long-term objective of becoming the

world's dominant economic power by 2049, the 100th anniversary of Mao's revolution.[26]

In pursuit of these considerations, China has turned the Internet into an instrument of social control, establishing, inter alia, a "Great Firewall of China" (the ability to monitor all on-line activity and disconnect all Chinese networks, or those in given regions, from the rest of the global Internet). It also imposes various restrictions on domestic and foreign companies in the cyber realm: Internet providers, for example, are required to keep servers handling Chinese traffic in China itself, where they are subject to state control.[27]

The Cyberspace Administration of China (CAC), which reports to the Communist Party's Central Committee, was established in 2014 to centralize national control over digital policy, including Internet censorship and propaganda. The CAC employs vast numbers of people (hundreds of thousands according to some estimates) and advanced technologies to continually monitor digital news outlets and social media platforms. The objective is not just to prevent the free flow of information and suppress dissent but to create and disseminate narratives that serve state interests and reinforce state ideology, part of what China calls a "harmonious Internet" and the importance of "discourse power."[28]

The National Cyber Security Center (NCSC), which occupies a 15 square-mile campus in Wuhan, is a combined school, research lab, incubator, and talent cultivator. The NCSC houses seven different centers, including the National Cyber Security School, which was scheduled to graduate its first class of 1,300 students in 2022 and another 2,500 graduates the following year. The Talent Cultivation and Testing Center will offer courses and certifications for some 70,000 early and mid-career cyber security professionals every year. Together, these two components of the NCSC could train over half a million professionals within a decade, a vast number, though far less than the projected deficit of 1.4 million cyber security professionals. The NCSC also includes centers focusing on research and entrepreneurship and two government laboratories.[29]

State-linked Chinese firms are building a global mass surveillance system. Using artificial intelligence (AI), the system is designed to link information and communications equipment, cameras, facial recognition software, and massive data sets on private citizens, to whom it assigns behavior-based "social credit" scores. As such, it will provide China with unprecedented power to surveil and affect the lives of individuals at home and abroad, including political opponents, and to micro-target propaganda tailored to personal data and search history. China also makes use of government-subsidized technology to promote the wiring of countries around the world with 5G wireless networks and undersea communications cables. Both are designed to make these countries increasingly dependent on China and its policies, including its authoritarian model of governance, and will further enable the collection of huge amounts of data. China

also exports surveillance systems of this sort, fueling a global trend toward digital authoritarianism.[30]

China often uses cyber means to strengthen its control over religious groups suspected of undermining the control of the Communist Party and of threatening national security, including Buddhists, Falun Gong, and Christians. The Uighurs, in particular, a deeply persecuted Muslim minority in the western province of Xinjiang, have been subjected to such all-encompassing monitoring.[31]

Coercion is used to control Internet discourse not just in China itself but also outside its borders. Foreign firms and organizations are pressed to avoid "sensitive" topics if they wish to operate in China. In 2019, for example, the manager of a National Basketball Association (NBA) team expressed support on Twitter for protests in Hong Kong. China responded by cutting off all ties with the NBA, which was quickly forced to apologize in order to preserve its access to the Chinese market. Similar cases have also occurred involving Marriott, Mercedes-Benz, and airlines.[32]

CNA attacks—in pursuit of economic advantage, Chinese affiliated hackers have conducted massive cyber attacks against technology firms and financial institutions in the United States, Japan, and Europe, leading a former director of the NSA to warn of "the greatest transfer of wealth in history," estimated to be worth trillions of dollars.[33] AFL-CIO computers have been breached in order to access information regarding the negotiations over the Transpacific Partnership, a trade deal that excluded China.[34]

China (as well as Russia) is thought to have inserted viruses into various models of US civil and military aircraft, potentially allowing external disruption of their controls, to cause crashes.[35] China may also have the ability to cause localized disruptions of critical US infrastructure that could last for days or weeks. Chinese-backed hackers targeted, and in many cases breached, the industrial control networks of nearly two dozen US oil and gas pipelines to prepare the ground for future attacks capable of taking control of the systems.[36]

In 2020 a small border incident between Chinese and Indian troops in the Himalayas reportedly led to a Chinese cyber attack against the electric grid of Mumbai, a city of 20 million people. Trains shut down, the stock market closed, and hospitals had to switch to emergency generators to keep ventilators going amid the coronavirus outbreak. In practice, Chinese hackers had apparently gained footholds in nearly a dozen critical nodes across the Indian power grid, not just Mumbai. The attack demonstrated how nuclear powers, desirous of avoiding the devastating consequences of a nuclear clash, can use cyber attacks as a more acceptable means of limited warfare and a way to gain strategic and psychological advantage.[37]

CNE attacks—China makes extensive use of the cyber realm for espionage purposes, especially in the US, where it may be the most active foreign actor.[38] In

2014 China stole the personnel files of 22 million federal employees, including sensitive data for security clearances. Of even greater consequence, China has hacked the weapons programs for the F35 fighter, Blackhawk helicopters, drones, AEGIS and Patriot anti-missile systems, and the US Navy's littoral combat ships, among other major weapons programs—the pride of US military technology.[39]

A Chinese hacking group apparently succeeded in first capturing code from an attack launched by the NSA against it and subsequently using that code against other countries and private firms. Some of the same NSA hacking tools were later dumped on the Internet and used by North Korean hackers in the WannaCry attack against the British health service (described in the section on North Korea later in this chapter) and in the Russian NotPetya attack on Ukraine.[40] In another case, China hacked a Google server containing court orders issued by the US Foreign Intelligence Surveillance Court, thereby learning who among its spies in the United States had been compromised.[41]

A relatively unsophisticated attack against governmental systems in Cyprus provided Chinese hackers with access to an entire EU diplomatic communications network. Over a period of three years, the hackers were able to download thousands of (low-level) classified cables dealing with European concerns regarding the Trump administration, the confrontations with Russia and China, the risks of a renewed Iranian nuclear program, and memorandums of conversations with leaders of Israel and Saudi Arabia. Still other hackers gained access to information regarding private meetings between the UN Secretary General and Asian leaders in 2016, at a time when North Korea was actively testing missiles.[42]

In 2020 Chinese hackers conducted a spear phishing attack against the Vatican's email system in order to gain information on its positions regarding the historic negotiations then underway over the appointment of Catholic bishops in China. The hackers also targeted the email system of the Vatican's office in Hong Kong, apparently to monitor its views on the protests there and its suspected support for demonstrators.[43]

In 2021, just weeks after the Russian SolarWinds attack was discovered, another cyber attack of global proportions came to light. Chinese government-affiliated hackers breached Microsoft Exchange, a program used to operate organizations' in-house email servers. At least 30,000 public and private entities in the United States alone were affected, including defense contractors and government agencies. In order to avoid detection by US intelligence agencies, which are barred from monitoring domestic computer systems, the Chinese hackers made use of servers rented under assumed identities in the United States, much as the Russian hackers had done in the SolarWinds attack. Once again, the attack was discovered by a private firm, not US defense agencies. The Biden administration, anxious to avoid an escalation of sanctions and counter-sanctions with

China, chose to respond by rallying a group of allies to publicly condemn Beijing for the attack, without imposing any actual consequences.[44]

CNI attacks—in 2008, long before Russia had begun its cyber campaign against US elections, China had hacked the presidential campaigns of Barack Obama and John McCain[45] and subsequently worked to gain access to the communications, speeches, and position papers of the new administration's top officials. In 2020 China considered conducting an information operation to affect that elections' outcome, but ultimately appears to have concluded that the outcome would not be sufficiently advantageous to justify the costs of potential exposure.[46] China has reportedly also interfered in elections in Cambodia, Taiwan, and elsewhere.[47]

Little better demonstrates China's approach to cyber information operations than the enormous effort made to hide, suppress, and subsequently shape Internet discourse, both in China itself and abroad, especially following the outbreak of the Covid pandemic and protests in Hong Kong in 2020. To this end, the CAC and local authorities issued thousands of strict and highly detailed commands regarding the content and tone of news coverage and directed paid trolls to inundate social media with appropriate messaging.[48] For China, "informationized operations," in which information is to be exploited and manipulated, are to become the main form of operations and primary factor in achieving victory.[49]

Chinese attacks against the United States repeatedly demonstrated the effectiveness of the cyber realm as an instrument of below-the-radar, deniable, asymmetric conflict. The United States always had countervailing interests that superseded the need to respond: the State Department needed Chinese help on North Korea; the Treasury did not want to upset the bond markets; the markets did not want a trade war. As a result, the United States repeatedly refrained from naming China, even when caught in significant attacks, and the Chinese themselves always responded with a scripted denial.[50]

North Korean Cyber Attacks

North Korea views any means of facilitating communications between its people, or providing access to external cultural and political influences, as a potential threat to the future longevity of the regime, its number one priority. Internet access in North Korea is strictly limited, therefore, to a small number of trusted people, with no access allowed for the vast majority of the population.[†51]

Conversely, North Korea considers the cyber realm a relatively cheap asymmetric means of leveling the playing field with the United States. Unlike kinetic weapons, cyber attacks can be launched covertly from anywhere around the

[†] A very limited number of people have access to an *Intranet* that cannot access outside websites.

world and are less likely to elicit a devastating US response. Moreover, North Korea's own cyber infrastructure is so underdeveloped that it presents few targets for counterattack, meaning that it can essentially act with impunity in the cyber realm to steal military plans and technology and to identify vulnerabilities in its adversaries' critical infrastructure for future use. To this end, North Korea has invested heavily in hacking and computer science and has reportedly developed a 6,000 strong cyber army that is focused, first and foremost, on gaining data critical for nuclear warhead miniaturization and ballistic missile technology, as well as launching ransomware attacks to gain funds for its nuclear program. Nevertheless, North Korea's overall cyber capabilities are still assessed as limited, and it is especially thought to lack sophisticated capabilities for purposes of cyber offense or intelligence operations.[52]

CNA attacks—in 2015 North Korea damaged two thirds of Sony Pictures' corporate computer network and issued violent threats against Sony and any theater that showed a satirical movie about North Korea. It further warned that it would take "decisive and merciless countermeasures" if the US government supported the film's release. The Obama administration viewed North Korea's demand as a form of political extortion and Sony's subsequent capitulation and cancellation of the film a dangerous precedent that might encourage others to launch cyber attacks against US entities for similar purposes.

The Sony attack highlighted the attribution problem in the cyber realm. Had it been a kinetic strike, attribution would have been comparably straightforward. The US intelligence community was adamantly opposed, however, to disclosure of the implants it had placed in North Korea's computer systems, and without the vital intelligence they provided, the administration could not publicly prove the North's culpability. In these circumstances, and desirous of avoiding further escalation, the administration decided merely to name and shame North Korea, stating that a proportional response would come at a time and place of US choosing. Shortly thereafter, North Korea's internet service was disrupted for several days. The United States never claimed responsibility.[53]

In 2015 North Korea launched cyber attacks against banks and broadcasters in South Korea, erasing the hard disks of roughly 48,000 computers[54] and in 2016 began using cyber crime to finance its ballistic missile program. An attempt to steal $1 billion from the Central Bank of Bangladesh failed when a simple spelling error in a bank order caused suspicion and led to the suspension of further transfers, after North Korea had absconded with just $81 million.[55] North Korea however, began using increasingly sophisticated technology to steal from banks and cryptocurrency exchanges and by mid-2019 had managed to steal over $2 billion for its weapons programs, including weapons of mass destruction.[56] By mid-2020 it had attacked banks in 38 countries, in some cases as many as 30 at a time.[57]

In 2017 North Korea launched WannaCry, a ransomware attack that spread to 230,000 computers in nearly 100 countries in just 48 hours, an unprecedented rate. The attack started with the British National Health Service, which was forced to shut down non-emergency services after computers in 20% of the hospitals in the UK had been infected. In Spain, WannaCry gained control over the computers of the largest telecommunications company. As it continued to spread, WannaCry infected a Chinese airline and even Russia's Interior Ministry. An unknown number of victims agreed to pay the $300 ransom for the key to unlock their data, but this key was never provided. Two factors made WannaCry particularly worrisome: the use of vulnerabilities in Microsoft software, originally stolen from the NSA by Russian hackers for purposes of ransomware; and the fact that in this case the ransomware, which is usually delivered to one user at a time, infected an entire network with a single click. The attack was ultimately terminated not by any governmental action, but by an alert individual.[58]

CNE attacks—in 2015 North Korea attempted to steal data from the operator of South Korean nuclear power plants, raising concerns regarding their safety,[59] and breached the South's nuclear research agency in 2021.[60] In 2016 North Korea breached a South Korean military computer system containing detailed US war plans, including decapitation strikes against the North, destruction of much of its mobile missile fleet, and seizure of as many of its nuclear weapons as possible. The North Koreans may have also planted "digital sleeper cells" in critical infrastructure in the South, ready for use should they wish to paralyze power supplies or command and control systems in the future.[61]

US Cyber Attacks

The United States has openly declared its determination to dominate the military cyber realm and is one of the most aggressive actors in this area.[62]

CNA attacks—the US has reportedly gained access to China's national command and control systems, including those for its nuclear weapons.[63] It has also planted malware in Russia's electric grid, apparently in retaliation for Russian breaches of the US grid, water treatment facilities, and nuclear power plants, in the forlorn hope that this would deter Russia from further cyber attacks against the United States.[64] At the height of the Syrian civil war, the NSA and Cyber Command presented President Obama with a sophisticated cyber attack designed to turn off electric power at key facilities in Damascus and other parts of Syria and essentially ground the Syrian Air Force, thereby preventing it from operating against opposition forces.[65]

The US has conducted cyber attacks against Iran on a number of occasions. The best known, Stuxnet, was actually part of a much broader cyber campaign,

Olympic Games, which was designed to provide the United States with the capability to shut down the Iranian economy at will (see detailed description in Chapter 10).[66] The United States also placed malware on Iranian computer networks in preparation for possible preemptive strikes on airbases, communication systems, and power grids[67] and has attempted cyber sabotage against Iran's missile program. In 2019, in response to Iranian attacks on tankers in the Persian Gulf and the downing of a US spy drone, the United States launched cyber attacks that destroyed a key database and military communications networks used by the Iranian Revolutionary Guards Corps (IRGC).[68] Just a few months later, in response to a missile and drone attack against Saudi oil facilities, attributed by both the United States and the Saudis to Iran, the United States launched a cyber attack designed to limit Iran's ability to spread propaganda, apparently damaging physical hardware in the process.[69] A harsher option, to shut down Iranian oil fields and refineries, was reportedly rejected for its potentially escalatory consequences.[70] The United States has also conducted cyber attacks against Iranian proxies, including Hezbollah in Lebanon[71] and Kata'ib Hezbollah, which operates in Iraq, Syria, and Iran.[72]

In 2016 the United States launched cyber attacks against ISIS, designed to disrupt its ability to convey orders from commanders, disseminate messages, attract new adherents, carry out day-to-day functions such as paying fighters, and most ambitiously, bring down its entire media operation. Dubbed Glowing Symphony, the campaign was the largest US cyber effort against ISIS and the first time it had ever publicly acknowledged a cyber operation against a foreign entity. In practice, the effects achieved proved transient and ISIS was able to rapidly renew most of its operations.[73]

North Korea's missile and nuclear programs present the United States with an even more complex set of challenges than Iran's programs. Unlike Iran, North Korea already possesses nuclear weapons, and its missile program threatens to provide it with the capability to strike the US homeland. A direct US military attack against North Korea would risk a nuclear exchange and the destruction of South Korea, and possibly Japan, and is therefore not a viable option. Instead, the Obama administration opted for a cyber sabotage operation designed to disrupt North Korean missile launches. Seven out of eight North Korean missile tests in 2016 crashed just seconds after launch, leading to the tests' suspension. Questions were subsequently raised whether the crashes truly were due to the US cyber campaign or to a variety of other potential causes. Whatever the reason, the North recovered rapidly and unveiled an entirely new missile program.[74]

Following Russian interference in the 2016 presidential campaign, the United States began a broad inter-agency effort designed to prevent future foreign meddling in the US political system and to impose costs on those who might seek to do so. During the 2018 midterm Congressional elections US

Cyber Command attacked Russia's Internet Research Agency, a digital propaganda facility operating from St. Petersburg, and disabled its systems for several days.[75] It also sent targeted messages to specific Russian cyber operatives and elites believed to be involved in the attack on the US elections, in effect warning them that their identities were known and could be publicized. In 2020 Cyber Command disrupted the world's largest botnet—over 1 million hijacked computers run by Russian affiliated hackers—which it feared would be used for ransomware attacks to disrupt US elections that year. To this end, Cyber Command used its authority to operate on foreign networks to discover malware and thwart malicious activity before it could have an impact. Part of the US strategy of "persistent engagement," the effort included "defending forward" in order to expose the adversary's capabilities, tactics, and code and to impose costs, whether in the form of time, money, or freedom of movement.[76]

CNE attacks—cyber espionage has become the primary means by which the United States collects intelligence on friends, enemies, and potential adversaries, in essence, virtually every country.[77] The NSA scours the world's software, hardware, and networking equipment in search of vulnerabilities through which to hack computer systems. It also makes use of its secret access to the transnational cables carrying Internet traffic worldwide and to data from Internet companies such as Google and telecommunications giants such as AT&T. The NSA is particularly focused on new zero day exploits, with thousands stockpiled for potential use against China alone. As early as 2013, the United States had reportedly implanted exploits in at least 85,000 computer systems in 89 different countries.[78] This number has presumably increased since then by orders of magnitude.

In 2015, following a massacre at a French music hall, the United States and France obtained court orders forcing Facebook to hand over information containing the smartphone numbers of the suspected terrorists, which were then used to triangulate their location. Hundreds were soon arrested.[79]

We now turn to the cyber threat to Israel.

3

Goldilocks and Other Cyber Quandaries

In the 21st century we have seen a tendency towards blurring the lines between the state of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.

Valery Gerasimov, Russian Chief of Staff

I chose to be proportionate. The United States is not looking to kick off a cycle of escalation and conflict with Russia [in response to SolarWinds attack].

Joe Biden, President of the United States

The cyber realm is still comparatively new and there is widespread concern that it presents a particularly dangerous set of capabilities that will prove extremely difficult to address.[1] Similar concerns have been expressed throughout history during earlier periods of technological disruption and consequent changes in military capabilities. Indeed, military history from time immemorial is replete with cases of time lags between the emergence of new technologies and operational capabilities and the development of effective responses. In the interim, the outlook has always looked grim, even insurmountable, for those seeking to cope with the new changes.

In the Introduction we sought to identify those attributes of the cyber realm that are significantly different from other realms, even unique, as well as to highlight areas of continuity. Chapter 1 then provided an overview of the global cyber threat. On this basis, we can now dive in deeper and address some of the most important theoretical and policy quandaries of concern to scholars and practitioners alike in the cyber realm. The discussion focuses, first and foremost, on strategic issues stemming from a realist approach.

The chapter presents 10 such quandaries, notably the difficulties states encounter in trying to achieve deterrence and to defeat adversaries in the cyber realm, the comparatively escalatory or non-escalatory nature of the cyber realm, and whether it is offense or defense-dominant. The final and most important

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0004

quandary, the cyber realm's actual impact on state power, military might, warfare, and statecraft, seeks to place the entire discussion in a broader strategic context.

The discussion of these strategic quandaries has two purposes, over and above their contribution to a heightened appreciation of the complexities of the cyber realm. The first is to provide background and inform our understanding of the thinking behind the decisions made by the government, IDF, and intelligence agencies in developing Israel's civil and military cyber capabilities, as presented in the following chapters. The second is to provide a basis for the conclusions we have drawn regarding the Israeli experience in the cyber realm to date, presented in Chapter 11, and for our proposal for a comprehensive Israeli cyber strategy in Chapter 12.

In most cases, the discussion of the quandaries is divided into two parts, designed to present both sides of the debate: the argument and the counterargument. We begin, however, with a brief discussion of how to conceptualize military cyber affairs.

Quandary 1: How to Conceptualize the Military Cyber Realm

Classic military thinking typically revolved around the "4Ds"—detection (i.e., early warning), deterrence, defense, and defeat. In recent times, the concept of resilience—the ability to bounce back from an attack and rapidly return to the antecedent level of functioning—has also come into widespread use. The United States applied a modified 4Ds approach to the asymmetric threat of terrorism in its National Strategy for Combating Terrorism: deny, diminish, defend, and defeat. Defense and defeat of terrorism were to be achieved, inter alia, by improved threat detection, while prevention of state sponsorship of terrorist organizations, defense of the homeland, and defeat of terrorists before they could attack were all designed to buttress deterrence.[2] The UK explicitly adopted a 3Ds approach in its 2016 National Cyber Security Strategy—detect, deter, and defend—which it changed to detect, disrupt, and deter in the 2022 iteration,[3] notably without defeat in either case. Israel based its defense strategy for decades on a 3Ds model of detection, deterrence and defeat and only later introduced the fourth D, defense, in the mid-2000s.[4]

In recent years, a plethora of new terms have emerged in various national cyber strategies and in the theoretical literature, including:

- Identification and attribution—often used instead of *detection*.

- Protection—used to refer both to *detection* and *defense*.
- Prevention and response—used to cover almost the entire gamut of older terms, including *detection*, *deterrence*, *defense*, and *defeat*.
- Protection, disruption, and degradation—used for *defense*.
- Superiority—used instead of *defeat*, although some documents speak of winning cyber conflicts.
- Resilience—used to cover *deterrence*, *defense*, *and defeat*.[5]

The significant technological and strategic changes wrought by the cyber realm notwithstanding, the dangers it poses are not so fundamentally different from already existing asymmetric threats that a new form of conceptualization is required, at least when addressing threats at the strategic level. Moreover, as just noted, some of the new terms blend a number of the classic ones, at times creating greater conceptual ambiguity rather than clarity. At least at this point in time, these new terms do not appear to have been sufficiently explicated to justify a collective jettisoning of the classic terms. This book thus makes extensive use of the latter, with some necessary adjustments.

The basic concepts behind the 4Ds and resilience have the advantage of being well understood and widely applied both by experts and governments around the world, although usage of the different terms does vary at times. Conceptually, the first three Ds (detection, deterrence, defense) and resilience are easily applied to the cyber realm, if difficult to achieve in practice. Defeat is more difficult to define in the cyber realm, and certainly to achieve, much as it is in regard to the asymmetric threats of terrorism and insurgency. We thus suggest a different and practical definition of cyber defeat later in the chapter. Importantly, the 4D's and resilience are not entirely discreet notions, but are strongly interrelated and mutually supporting.

Quandary 2: Is Cyber Deterrence Feasible?

Deterrence refers to the ability to harm assets of importance to an adversary in order to affect its cost/benefit calculus and thereby dissuade it from taking unwanted action.[6] Cyber deterrence, accordingly, refers to the ability to use cyber means as a way of affecting the adversary's cost/benefit analysis for similar purposes.[7] For deterrence to be effective, an adversary must have assets, or values, to which it attaches significance and the deterring state must be perceived as having the ability to adversely affect them. Deterrence is dynamic and evolves constantly as actors develop their capabilities, counter-capabilities, and deterrent postures. We begin with a general discussion of the concept of deterrence

before turning to the primary quandary in this area, whether deterrence can or cannot be achieved in the cyber realm.

Deterrence can be pursued either through denial (prevention) or retaliation (punishment). The two approaches are not mutually exclusive and can be pursued concomitantly.

Deterrence by denial—may be achieved through an actual demonstration, or credible signal, of a state's ability to prevent an adversary from taking a certain action, thereby undermining its confidence in the utility of trying to do so to begin with. Offensively, deterrence by denial can be achieved by attacking an adversary's *counter-force* targets, that is, significant military capabilities,[8] or through a variety of operations designed to preempt and degrade them. The Stuxnet cyber attack on Iran's nuclear program and US attempts to sabotage the ballistic missile programs of North Korea and Iran by cyber means are examples of offensive cyber deterrence by denial. Defensively, deterrence by denial can be achieved through an increase in system and network security.[9] China's "Great Firewall" and Iran's National Information Network, which largely isolate their national networks from the rest of the Internet, are more extreme versions of defensive cyber deterrence by denial.

Deterrence by retaliation—is based on the threat to punish the other side either by causing significant harm to assets or values that it holds dear, known as *counter-value* targets, for example, population centers and economic capabilities, or by making the costs of taking action higher than the expected utility. Examples of cyber deterrence through punishment include Russia's attacks on Estonia, Georgia, and especially Ukraine (Chapter 2). Some military capabilities may be of such importance that they come to constitute counter-value targets in their own right, and a variety of capabilities straddle the two categories, for example, power stations and civilian communications systems, which serve both the civil and military sectors.[10]

The Argument: Cyber Deterrence Is Not Feasible—considerable skepticism exists among academic scholars regarding the applicability of deterrence to the cyber realm. Indeed, the very prevalence of cyber attacks is held to be proof that they cannot be deterred.[11] A number of factors explain why this may be the case.

First, as a new domain of warfare, the level of uncertainty regarding cyber weapons is still high.[12] A deterring state may successfully penetrate an adversary's networks but not know that the intrusion has been detected and the route of access blocked. The target may not know that it has been attacked and even suffered damage, and the attacker may have a far harder time assessing what damage, if any, it has actually caused. In conditions such as these, deterrence by denial is of limited efficacy. Similarly, if the adversary is unaware of the deterring state's

capacity to inflict the promised punishment, deterrence by retaliation is also of limited utility.[13]

As in other areas of international affairs, perception is crucial to deterrence, in which both sides assess the other's likely behaviors and formulate their policies accordingly, in the knowledge that the other is doing the same in regard to them. Good intelligence is critical. The deterrer must be able to understand how it is perceived by the adversary, what the adversary values and how it is likely to respond to its actions.[14] Often, however, deterrence is undermined by failures of perception. The deterring state is likely to believe that the adversary perceives it accurately, or as it sees itself, even though this is frequently not the case. Indeed, leaders often fail to understand just how menacing they appear to their adversaries, or the extent to which actions they perceive as benign are viewed by adversaries as threats to their vital interests.[15] It is also very hard to distinguish between CNE attacks (cyber espionage) and CNA attacks (disruption and destruction). Unlike the conventional and nonconventional realms, in which deterrence is based on avoidance of operational contact, the cyber realm is continually contested,[16] further increasing the level of uncertainty and making deterrence that much more difficult.

Deterrent strategies are based on three primary elements: *capability*, *credibility*, and *communication*.[17] In the conventional and unconventional realms, states can credibly bolster their deterrence by developing, testing, and deploying weapons and can communicate this to adversaries through overt and covert means. In the cyber realm, in contrast, the secrecy needed to preserve the effectiveness of weapons means that states are far more constrained in their ability to do this. States can hardly display malicious code in a military parade, defense exhibition, or military exercise. The very acknowledgment that a cyber capability exists risks alerting the adversary to the vulnerability to be exploited.[18]

Deterrence worked well in the nuclear realm because both the United States and the USSR (or Russia today) knew that they had a guaranteed ability to destroy each other, even after absorbing a first strike: mutually assured destruction (aptly known as MAD). Deterrence derived from the shared certainty that the consequences of a nuclear attack were intolerable and that no defenses could ever sufficiently mitigate their destructive power. Both sides also had confidence in the integrity of their command and control systems and weapons. In the cyber realm, in contrast, the actual effects of cyber weapons remain largely unknown, effective defense should be feasible even against advanced capabilities, and confidence in the integrity of command and control and weapons systems is limited. The "escalatory ladder" regarding cyber weapons also remains unclear. Whereas it was obvious that nuclear weapons were more escalatory than conventional ones, it is unclear how cyber weapons fit in relative to others.[19]

A further complication surrounds the issue of deterring terrorist groups in the cyber realm. As in the physical realm, the damage they can cause is painful, but usually limited. Conversely, their tolerance for punishment may exceed the deterring state's willingness to mete it out or risk further harm to itself. This is especially true of Western democracies, including Israel. It is not that they are incapable of defeating terrorists and insurgencies but that the human, economic, and other costs associated with this, to themselves and to their adversaries, may not be commensurate with the actual gravity of the threat.[20]

A state's level of cyber dependency, that is, the degree to which it relies on computer systems and networks to function, can also have a major influence on its deterrent posture. States with high cyber dependence are more vulnerable to attack and thus to deterrent measures than those whose cyber dependence is lower,[21] and unless they reduce their level of vulnerability, they risk the danger of self-deterrence. Knowledge of the damage that other actors could cause them, including those with low cyber dependence, might make them reluctant to utilize either their cyber or kinetic capabilities. For example, a national leader might be hesitant to act if a power blackout caused by an adversary in one major city was likely to be spread to additional cities in retaliation.[22]

To date, the most cyber capable nations have stayed well below the threshold of full cyber warfare. Cyber deterrence below that level, however, has proven elusive.[23] Indeed, deterrence is essentially irrelevant for purposes of preventing espionage and information operations (CNE and CNI attacks).

The Counter Argument: Cyber Deterrence Is Feasible—in contrast with this skepticism expressed by academic experts, the US, UK, and NATO cyber strategies are based on the shared belief that the principles of deterrence are as applicable to the cyber realm as to the physical.[24] The National Security Strategy of the United States emphasizes that "the US will impose swift and costly consequences against actors who undertake significant malicious cyber activities"[25] and both the US and UK national cyber strategies specifically identify deterrence as a top priority.[26] NATO has concluded that investing in cyber capabilities in a way that is visible to opponents can communicate resolve and make deterrence more credible, as can demonstrating capabilities in real-world situations.[27]

To achieve effective deterrence, actors must make clear to adversaries what their capabilities and intentions are and the consequences they are likely to suffer.[28] As noted, this is difficult to do in the cyber realm, meaning that the clarity and consequent credibility that buttress traditional deterrence are harder to achieve.[29] States will, however, have to find different ways to communicate their capabilities and intentions,[30] including public deterrent statements and postures and messages through confidential channels.[31]

Healey distinguishes between four primary means of achieving deterrence in the cyber realm: *Explicit deterrent postures* designed to convey resolve and the ability to deliver punishment, for example, by threatening to shut off an adversary's electric grid. *Indirect deterrent postures* based on the adversary's knowledge of the overall size and strength of the deterring state's cyber capabilities. *Quiet signaling* to convey to the adversary that something that it values is at risk, especially if the intrusion is already in place in the adversary's system. *Symmetric responses* that match an adversary's known or suspected cyber capabilities, such as parallel intrusions into its electric grid. Healey believes that the explicit and indirect deterrent postures should be stabilizing, because the deterring side's capabilities are known to its adversaries and are thus credible. The quiet and symmetric responses may be less stabilizing, because the deterrent threats are tailored to specific adversaries, who may, or may not, be aware of them.[32]

States can buttress their deterrence by emphasizing the strength of their overall national capabilities in the cyber realm. The better developed a state's cyber ecosystem, strategy, and institutions and the more robust its posture, the better adversaries will be able to deduce its deterrent capabilities. Fortunately for the deterring side, capabilities do not have to be completely credible in order to be effective. Credibility is subjective, and it is the target that determines whether a deterrent threat is more or less credible than the deterring state believed. In practice, cyber threats may be more credible than kinetic ones, simply because they are more likely to actually be used.[33]

Deterrence is deeply linked to the other 3Ds and to resilience. For deterrence to be effective, detection and attribution must be possible, including an identifiable "return address" for the deterring side to retaliate against. Improved defenses reduce the attacker's prospects of success and raise its potential costs, thereby leading to a commensurate reduction in the attractiveness of attacking and strengthening deterrence. Indeed, nothing concentrates a potential attacker's mind and increases deterrence more than the prospect of defeat. Resilient systems can be restarted rapidly, further reducing the potential benefits to the attacker.[34]

Standalone cyber deterrence is probably not truly feasible, or at least has not proven so to date. Rather, cyber deterrence can and usually should be integrated into the full range of diplomatic, economic, and kinetic responses available to the deterring state, whether for purposes of denial and/or punishment, otherwise known as "cross-domain" deterrence.[35] Cross-domain deterrence may be especially effective when combined with a strategy of "cumulative deterrence," that is, repeated frustration of the adversary's attempts to achieve its objectives, thereby leading to a sense of futility and to a decision on its part to forgo further attacks, in practice, deterrence by denial.[36] Cumulative deterrence is better suited to cases where the deterring party does not have the ability to deliver a

single or small number of devastating blows that are likely to bring the conflict to an end, for example, in asymmetric threats such as terrorism and cyber. The downside with cumulative processes, of course, is that they take time.

A state seeking to strengthen its deterrence can adopt a declaratory posture that sets out the types of attacks that will trigger a response, the response threshold, and the planned retaliatory measures.[37] In extreme cases in the physical realm, such as a nuclear attack, in which the national leadership may not be available to issue orders in a timely fashion or at all, states have also been forced to formulate ex-ante declaratory policies: if an attack of such and such nature occurs, it will respond automatically in a predetermined manner. Also known as pre-delegation, lower echelons are granted the authority to issue certain kinds of orders, in clearly defined circumstances, which the national leadership would presumably have given were it able to do so. Declaratory policies such as these must be based, by necessity, on judgment calls regarding the party presumed to be responsible and are knowingly based on only partial information and preexisting assumptions, with all of the attendant pitfalls. When faced with potentially disastrous cyber attacks, states may have no choice but to adopt similar approaches, including predetermined automated responses.[38]

A further issue of considerable importance in cyber deterrence, as with kinetic, is that of symmetry and proportionality. The United States and UK maintain the right to use kinetic force in response to cyber attacks, that is, to respond asymmetrically.[39] Proportionality, in contrast, continues to be an international expectation, much as in the physical realm. Effective deterrence by punishment thus requires that a state have credible and scalable capabilities covering the entire range of responses available to it, kinetic, cyber, diplomatic, economic, and more, at all levels of conflict.[40]

Quandary 3: Are Cyber Detection and Attribution Still a Severe Problem?

Intelligence regarding an adversary's capabilities and intentions—and early warning of impending attacks—are as critical in the cyber realm as in the physical. Given the immediacy and pervasiveness of cyber attacks, they may be more so. Indeed, deterrence, defense, and defeat of an adversary all depend on the ability to reliably detect attacks and assign culpability in a timely fashion.

The Argument: Attribution Is a Severe Problem—the cyber realm presents some particularly challenging problems of detection. Unlike attacks in the physical realm, cyber attacks do not require the movement of troops and physical assets and can be disguised far more easily, making it difficult to determine if an

attack is underway or has even taken place. Cyber weapons rarely leave smoking ruins and the sheer number of potential attackers dispersed around the globe—state, nonstate, group, and even individual—presents a unique challenge to the monitoring and attribution capabilities needed for detection. Botnets (which can include millions of computers), proxy sites dedicated to anonymizing, and other technologies further complicate matters.[41]

In 2020 the SolarWinds and Microsoft Exchange attacks, attributed to Russian and Chinese affiliated hackers, respectively, targeted tens of thousands of users each, including sensitive government agencies in the United States and elsewhere. Despite the vast investments made by the US and other governments in cyber security during the previous years, both attacks were first detected by private cyber security firms, bringing the detection challenge into particularly sharp relief.

Cyber attacks can be launched anywhere in the world, have numerous points of entry, and need to succeed only once to cause significant damage. Moreover, the increasingly interconnected nature of governmental, military, and commercial networks means that the latter can now be used as a gateway to attack the former, albeit usually the less sensitive ones. The private sector has thus become a source of vulnerability for governmental and military systems, further increasing the already growing need to provide early warning to major private sector actors, especially critical infrastructure ones.

Nonstate and state actors alike use the comparative anonymity of the cyber realm to their advantage to avoid attribution and retribution. Deception and plausible deniability are long-standing features of the strategies of asymmetric conflict favored by North Korea and Iran. Russia and China employ semi-private proxies to conduct cyber operations without leaving digital fingerprints. Even the United States chose not to take responsibility for its reported disruption of North Korea's Internet following the attack on Sony Pictures, nor attempts to sabotage both its and Iran's missile programs.[42]

The Counter Argument: Attribution Is Manageable—difficult as the attribution problem may be, it is manageable.[43] States and even private firms have rapidly improved their technological and forensic intelligence capabilities and consequently their ability to determine who is behind an attack. A state actor with sophisticated cyber capabilities, coupled with good intelligence and cooperation with other states, can make an adversary's attempts to hide its identity quite difficult.[44]

Technical indicators of the attacker's cyber capabilities, including the specialized capabilities required for more sophisticated attacks, limit the range of potential perpetrators. The apparent political and/or operational motivations

behind an attack further assist with attribution. Even if a state cannot pinpoint with high confidence who specifically carried out a given attack, factors such as these usually enable it to identify a comparatively small number of likely culprits.[45] The primary problem today is that reliable attribution takes time and is resource-intensive, but political developments may outpace the speed of technological and forensic capabilities.[46] In any event, attribution is ultimately a political decision, not a legal one.[47]

Some factors work to the defender's advantage. Whereas conventional and unconventional weapons are fungible and can be used against targets of all kinds, cyber weapons, at least advanced ones, are tailored to specific targets and can only be used against them. A sophisticated cyber weapon developed to attack an enemy's surface-to-air missile system, for example, is likely to be of no use against its surface-to-surface missiles, and even minor changes to an adversary's network can render a cyber weapon useless. Indeed, extensive intelligence is essential for both the development of sophisticated cyber weapons and their actual use.[48] For the defender, the tailored nature of cyber weapons at least somewhat eases the attribution challenge.

In some cases, attribution efforts are abetted by the attackers themselves. For instance, hacktivists typically seek publicity for their causes, organizations, or themselves and often make clear who is behind an attack.[49] Even then, however, attribution can still be problematic, since the individuals and organizations involved often do not use their real names or disclose information that would make it possible to identify them. The primary problem, of course, is attribution in cases where the attacker is a state or nonstate actor with sophisticated capabilities, which does not wish to be identified.

Force metrics, such as the number of programmers and other advanced personnel at the adversary's disposal, the size of its budgets, and its ability to synchronize the work of multiple complex teams, are critical in cyber detection. Even knowing where programmers were trained can provide important insights into the types of attack they are likely to develop.[50] Attackers often find it necessary to conduct cyber reconnaissance missions before launching attacks, to assess the weak points in the defender's systems, thereby providing additional opportunities for detection.[51] The larger a planned or ongoing cyber attack, the easier to intercept communications between attackers, detect capabilities and intentions, and defend against it.

Much as cyber technology poses new problems of detection, it also provides new options for doing so.[52] Vast numbers of cyber attacks can be launched simultaneously, but the technology can also be used to detect and counter a similarly large number, including a broad spectrum of autonomous

data collection, aggregation, and synthesis methods to improve constant monitoring of the adversary's capabilities and modus operandi. Attribution can still take time, but it is no longer true that cyber attacks do not have a "return address."[53]

Advanced nations have already taken a variety of measures to strengthen their detection capabilities, including placement of sensors around important networks, expanded information sharing with the private sector, and heightened international cooperation. Whereas the latter can be conducted through long-existing channels of intelligence and law enforcement cooperation, information sharing *within* states, between the government and public and private sector entities, remains a significant challenge, requiring complex legal, organizational, and political changes.[54]

For advanced states, attribution at the intelligence, if not legal, level usually no longer constitutes a major obstacle. The true detection challenge lies, therefore, not in the vast number of potential attackers around the globe but in a more limited and manageable number of highly sophisticated adversaries. It also lies in developing the intelligence capabilities necessary to accurately anticipate and prevent future attacks before they cause damage, rather than a post-facto "plugging-the-holes" approach toward attacks already in progress or over.[55]

Different levels of certainty are necessary for attribution depending on the state's preferred type of response. A comparatively low level of certainty is all that is required for purposes of quiet diplomacy. In such cases, a state could simply accuse another of having conducted a cyber attack without need for definitive proof. Greater certainty would be required before making public accusations. A still higher level of certainty would be necessary in order to undertake legal and especially retaliatory action, be it kinetic or cyber.

Once a state attributes an attack to a specific actor, especially if it does so publicly, it risks becoming overly committed to the need to respond and exact retribution, even when it does not necessarily have good options and might otherwise prefer to refrain from doing so. Paradoxically, however, the attribution challenge can also be an advantage in this regard. The difficulties involved in attributing culpability may provide for a measure of constructive ambiguity that broadens a state's freedom to choose whether and how to respond. Even if the state knows the attacker's identity, the attacker and other actors do not necessarily know this to be the case, thereby allowing it to avoid a potentially costly response without excessive reputational damage.[56]

States engage in a constant effort to assess where the next threats are most likely to come from—and these change very quickly in the cyber realm. The Australian national cyber strategy, for example, calls for improved detection through continuous real-time monitoring online.[57] Given the widespread skepticism about the efficacy of deterrence in the cyber realm, effective detection is particularly important.

Quandary 4: Goldilocks and the Cyber Escalation Question

In the pursuit of cyber deterrence, states face a conundrum similar to the one that Goldilocks encountered: how to choose a level of deterrence that is neither too cold nor too hot, but just right: in other words, how to calibrate their actions in a manner that is sufficient to dissuade an adversary from taking unwanted action but not so strong that it has little choice but to escalate.[58] Some experts believe that cyber attacks are inherently more escalatory than kinetic ones, others take precisely the opposite view. The jury is still out, but leaning in the latter direction.

The Argument: Cyber Is More Escalatory—in pursuit of their national security, states conduct cyber operations, including penetration of other states networks, and in so doing threaten their security. The result may be a "cyber security dilemma," an extrapolation from the classic concept of the security dilemma, resulting in an escalatory cycle and even war.[59]

Even defensively minded states may have a significant incentive to intrude into other states' networks, gather intelligence about their cyber capabilities and possible targets, or gain insights into the views and intentions of their leaders. The originating state may deem its moves to be benign, but adversaries may not share this perception and are likely to take countermeasures to prevent them, in turn prompting a response from the first state and further contributing to the escalatory cycle.[60] If the damage from an attack spreads to other systems or states, the defending state, or one of the other states affected, may feel the need to retaliate and escalate, even in cases where the original attack was not deemed sufficient to warrant this.[61]

Paradoxically, some of the cyber realm's primary advantages may actually exacerbate the risks of escalation. Cyber means can be used to accomplish military goals without having to resort to kinetic weapons and risk the lives of either side's military forces and civilian populations or cause physical damage. They can also be used to conduct highly pinpointed attacks, with minimal collateral damage.[62] These erstwhile advantages may actually serve to increase the temptation to use cyber weapons, or at least reduce the political and moral inhibitions against doing so, thereby increasing the dangers of escalation.[63] Moreover, unlike nuclear weapons, whose extraordinarily destructive consequences have rendered their use all but inconceivable, cyber weapons may be used far more readily, despite potentially systemic consequences. They can also be used in peace time.[64]

Experts who believe that the cyber realm is escalatory also tend to believe that offensive cyber capabilities will outpace defensive ones, thereby increasing the prospects of misperception and consequent escalation. The prospects of

misperception are further exacerbated by some of the other attributes of cyber attacks already noted, including the difficulty in distinguishing between defensive and offensive cyber operations and between those designed for intelligence collection and for offensive purposes; the fact that cyber attacks do not require the cumbersome and more easily detectable movements of conventional forces, thereby increasing the prospects of surprise; and the fact that they can be executed (although not planned and prepared) instantaneously, from a virtually unlimited number of sources, leaving leaders with little, if any, time to stop and deliberate prior to responding.[65]

There may be significant incentives to attacking first in the cyber realm. An assessment that a cyber attack is imminent could incentivize a state to launch a first strike out of fear that its cyber capabilities would be rendered ineffective ("use it or lose it"). Even a state that does not view a preemptive first strike as a preferred option may still perceive significant advantages in not going second. The ability to degrade or even disable an adversary's command and control systems, for example, would proffer great advantage and be particularly tempting. States may further deem it essential to act quickly and resolutely against emerging cyber threats to neutralize them before the adversary can retaliate, especially since cyber targets may only be vulnerable briefly before even minor changes to the adversary's system render their advanced offensive weapons ineffective.[66]

The fear of being attacked, exacerbated by the perception that the cyber realm favors offense, has led countries around the world to make massive investments in military cyber capabilities, thereby further increasing the risks of escalation.[67] If offense is, indeed, dominant in the cyber realm (see next quandary), similarly sized forces will prove insufficient for defensive purposes, thereby further contributing to arms races and escalatory cycles.[68] The growing adoption of active cyber defense strategies by the United States and other countries, in effect, aggressive automatic countermeasures, may also exacerbate escalatory dangers by decreasing states' ability to reduce tensions through deterrence or more limited countermeasures.[69]

Lastly, states have yet to reach an international consensus regarding accepted norms of behavior in the cyber realm, meaning that there are fewer constraints. Several forays into the field have been made, but creating international norms, agreements, and law has proven difficult and will take time, as states are loath to compromise their national interests.[70]

The Counter Argument: Cyber Is Less Escalatory—some experts believe that the cyber realm is less escalatory than the physical and that it even establishes a threshold that restrains the level of escalation. Partly, this is held to stem from the nature of cyber weapons, whose effects cannot be fully anticipated

before use and whose potentially unintended consequences may thus make decision makers hesitant to act in a manner that could lead to further escalation. This contention is further bolstered by the interconnected nature of military and civilian networks, including critical national infrastructure. Leaders will likely be more hesitant to risk an attack on an adversary's military targets if this could result in retaliation against their own critical infrastructure.[71]

Kinetic attacks can only remain "below the radar" or in the "gray zone" for which states do not take credit for so long. At a certain point, however, they can no longer be hidden or their effects downplayed, and they typically generate political pressures on a government to respond. Cyber attacks, in contrast, can remain in the gray zone and may only be known publicly to the extent that the leadership so wishes, thereby providing it with greater political leeway to choose whether and how to respond and increasing the prospects of quiet deterrence by punishment.[72] In the case of the cyber attack on Sony pictures, for example, the US intelligence community objected to the use of the strong evidence it had of North Korean culpability, leaving the administration unable to make an effective public case for a forceful response. It thus chose to respond, publicly, merely by "naming and shaming" North Korea, but disruptions to Internet service there in the following days were attributed in media reports to the United States.

The ability to use cyber attacks as signaling mechanisms, without causing physical damage, can offer rival states a way to avoid or de-escalate a conflict. States can choose to respond to intrusions with low-level or proportional attacks designed to dissuade additional attacks, halt a cyber conflict, and avoid further escalation.[73] US policymakers, for example, did not believe that Russia's intervention in the 2016 US elections warranted a military response and the diplomatic, legal, and economic options for deterring it from further action were deemed ineffective. Options to retaliate directly, by cyber means, were also scrapped, because the United States feared that Russia might escalate further and attack critical US infrastructure, such as the electric grid, in which it had already implanted malware. In 2021, following the massive SolarWinds attack, the United States again chose a "proportional" response to avoid escalation, as it did a few months later when it formed a coalition of allied states to condemn China for its attack against Microsoft Exchange without concrete consequence. Quiet Russian and Chinese cyber measures were thus classic cases of attacks that succeeded in curbing and deterring US responses and in avoiding escalation.[74] In early 2022, as Russia massed forces on Ukraine's borders, President Biden appeared to indicate that he would consider cyber attacks to be the equivalent of a "minor incursion" rather than a ground invasion and respond accordingly in a less escalatory fashion.[75]

One empirical study found that states do, indeed, tend to respond to cyber attacks with cyber means and in a proportional "tit-for-tat" manner, designed to reduce the prospects of escalation.[76] Since most cyber attacks do not cause physical damage, states apparently prefer to deal with the more limited virtual consequences, rather than escalate and potentially risk kinetic action. Moreover, studies of public opinion indicate that respondents clearly differentiate between cyber and kinetic responses. Even publics that tend to prefer hardline responses to other threats generally do not support escalation to the physical realm when diplomatic or cyber options are available.[77]

Given all this, some believe that cyber conflict should be viewed as a form of "tacit agreed competition," in which states' efforts to gain advantage over each, other actually result in tacit understandings regarding the acceptable range of conflict. Proponents of this approach further believe that a protracted process of adversarial interaction, possibly lasting decades, will lead to the establishment of accepted boundaries of behavior in the cyber realm, thereby preventing escalation to new levels of conflict and ultimately prove stabilizing. Others, unsurprisingly, reject this approach[78] and, in any event, few have decades to wait before finding out.

Arguably, the most important argument for the less escalatory nature of cyber attacks may simply be a practical and potentially transient one. To date, at least, most cyber attacks have not imposed a heavy enough cost on the victim to justify kinetic escalation.[79] Indeed, there are only three known cases in which states have employed kinetic means in response to cyber attacks: a US drone strike against ISIS in 2015; an Israeli airstrike on Hamas's cyber headquarters in 2019; and a further series of attacks during the round of fighting in 2021, in which Israel essentially destroyed all of Hamas's other cyber capabilities. In all three cases, the use of force was directed against a nonstate actor and did not lead to further escalation.[80] In contrast, states have responded to kinetic attacks with cyber attacks frequently, once again indicating the non-escalatory nature of the cyber realm.[81]

In the end, deterrence is a function of anticipated costs, not the means by which they are achieved. It should thus make little difference to an adversary whether a military capability is destroyed or a dam breached by cyber or kinetic means. The key question, from the perspective of the deterring state, is which threatened response is likely to be the most effective in achieving its objectives.[82] If the objective is to avoid further escalation, the threatened response to a cyber attack might be similar in kind, or at least in magnitude. If the objective is otherwise, escalation dominance, for example, the threatened punishment might increase significantly, subject to considerations of credibility, the predictability of expected effects, and the vulnerability of targets.[83]

Quandary 5: Is Cyber Offense-Dominant, Defense-Dominant, or Neither?

Power in the cyber ream is a function of a state's ability to control information resources, including the confidentiality, integrity, and availability of the information itself and of the systems that process, transmit, and store it. Offensive operations seek to damage the confidentiality, integrity, or availability of the adversary's information resources, whether for their intelligence value, for purposes of disruption or destruction, or to deprive the adversary of them, including those resources needed for offensive action. Defensive operations, in contrast, seek to preserve the confidentiality, integrity, and availability of the information resources under the defenders' control. Offense and defense in the cyber ream can thus be regarded as contests to gain or retain control over information resources.[84]

The Argument: Cyber Is Offense-Dominant—US strategy considers the cyber realm one of "continuous engagement," or what others prefer to call "persistent engagement." Either way, the cyber realm is a highly contested space, in which states seek to impose costs on each other and to compel the other to shift resources from the offense to defense.[85] This line of thinking then leads to a view of the cyber realm as an "offense-dominant," or "offense-persistent," strategic environment, in which the defense is destined to lose in the end.[86]

The cyber realm changes all of the time. Every new version of hardware and software, or system integration, creates new opportunities for the offense and places new demands on the defense, which is constantly forced to play catch-up and can provide no more than temporary respites from attack.[87] The defender may not even know that it has been attacked or is under attack, meaning that it may also not even know whom it must defend against. Moreover, the number of potential adversaries in the cyber realm is far greater than in the physical world, and each may have its own rapidly changing offensive capabilities and approaches.[88]

Some of the advantages of cyber attacks—speed of execution, relative anonymity and consequent impunity, cost-effectiveness, dearth of international cyber norms or regimes, and more—further incentivize a would-be attacker. Indeed, many observers today believe that cyber offense will continue to enjoy a significant advantage over defense for the foreseeable future at least. Moreover, as in other domains, the defender must effectively protect all important targets all of the time, whereas the intruder may only have to successfully breach one of them once. The attacker also enjoys the advantages of initiative and surprise, choosing the means, time, and location of the attack in a domain where speed and agility are particularly important.[89]

The Counter Argument: Cyber Is Defense-Dominant—others challenge the assumption of offensive dominance in the cyber realm. While recognizing that this may be true for simple forms of attack, proponents of this approach argue that developing sophisticated cyber exploits requires considerable investments in time, expertise, and expense, whereas the defenses required to thwart them may not. Indeed, comparatively simple and inexpensive changes to existing systems may be sufficient to frustrate even sophisticated attacks. The malleability of the cyber realm, that is, the ability to proactively and continually change network architecture, software, and processes, further favors the defense and may provide it with primacy. Even critical national infrastructure systems, commonly thought to be particularly vulnerable, are harder to attack than otherwise believed; they tend to be highly complex, have only limited interconnectivity, and are comparatively resilient due to redundancy measures. New technologies, such as big data, AI, and quantum computing, which provide for major improvements in automated defenses and communications security, may further swing the balance from the offense to the defense. The growth in private cyber security vendors, such as McAfee and Symantec, has made it even harder to conduct offensive cyber operations and strengthened defenses.[90]

A further challenge to the offense is the fact that many important systems are "air-gapped," that is, physically, electromagnetically, and electronically isolated from unsecure networks. Creating an effective air-gap can require sophisticated capabilities and is usually reserved only for critical systems, such as nuclear power plants, military networks, and some medical equipment.[91] Air-gaps provide considerable security, but can still be attacked by those with access to them, whether wittingly or unwittingly (if they unintentionally plug in an infected flash drive, for example). Stuxnet, for instance, reportedly targeted an air-gapped system. Other sources speak of tiny circuit boards and USBs inserted surreptitiously into target computers by the United States or one of its allies before being shipped out of the factory or while in transit.[92]

In short, it is premature to judge whether the cyber realm is offense or defense-dominant. It is probably more accurate to say that it is inherently neither[93] and that the relative advantages of cyber offense and defense will wax and wane, as has been the case with all other military technologies (with the partial exception of nuclear weapons) as capabilities and strategies evolve over time.

Quandary 6: Is Effective Cyber Defense Possible?

The debate about cyber defense, unlike most of the other quandaries, does not lend itself to a division into contending approaches, pro and con. All agree that

cyber defense is a significant challenge and differ only in the severity they attach to the problem and the means of addressing it.

Some networks have thousands or even tens of thousands of computers, with even greater numbers of constantly changing users and vast quantities of information stored in different parts of the system.[94] The size of this "attack surface" is critical in terms of the opportunities it provides to attackers. Most systems make little use of the general-purpose hardware and operating systems they are built on, which is where vulnerabilities are often found, or of the numerous applications that were needed at some point in the past, but subsequently fell into disuse.[95]

Cyber defense can be passive or active.

Passive defense—refers to measures taken *within* a defender's systems, including encryption, configuration monitoring and management, vulnerability assessment and mitigation, and general cyber hygiene (e.g., strong passwords and training personnel to avoid behaviors that may lead to breaches). Passive defenses are generic, in other words, they are not directed against a specific threat or actor.[96]

Active defense—can be conducted both within a defender's system and without.[97] Active cyber defenses *within* a defender's systems include firewalls, antivirus scanners, user account management software, authentication measures, human analysts to hunt down intruders, and a variety of automated and integrated technologies to identify, interdict, isolate, and remove threats at machine speed.[98] Since these measures take place within the defender's systems, and are usually taken by the agency, firm, or individual who owns the system, they raise few questions of domestic or international law. Cyber defenses conducted *outside* of a defenders' systems, conversely, raise complex domestic and/or international legal issues. External active cyber defenses are commonly, but inaccurately, equated with offensive operations and "hack backs" and are the subject of considerable controversy.[99]

Active defense has come to be the accepted modus operandi. US cyber strategy, for example, is based on *defending forward*, that is, preemptively acting to disrupt or halt malicious cyber activity *at the source*, before it can have an impact.[100] The UK cyber strategy speaks of active cyber defense measures to proactively combat, or defend against, cyber threats. NATO, too, has adopted an active defensive approach. The German strategy speaks of both passive and active defenses.[101]

Defense in the cyber realm, as in other areas of asymmetric conflict, is not a standalone concept but is inextricably linked to a state's ability to detect and deter threats and to its resilience. Not all targets can be defended, but particularly important ones can be hardened to the point that potential attackers come

to question whether their chances of success are so limited, or the defenders' ability to rapidly recover and bounce back so effective,[102] that they doubt the utility of attacking and do not even try—in effect, defeat through deterrence by denial.

Cyber weapons do not remain effective indefinitely, and it is impossible to predict how long they will do so. Security protocols and antivirus software can be improved, vulnerabilities discovered and patched, software updated, and hardware replaced. Studies have found that 90% of all intrusions could have been prevented had basic best practices in cyber security been observed, but it typically takes 100–128 days before patches are updated and other simple measures taken.[103] Given the difficulty in predicting when these changes will take place, the window of opportunity for an attack may also be inherently unpredictable, much like targeting mobile missile launchers in the physical world. Effective cyber defenses should not be limited to measures to harden the system, for example, identifying and patching vulnerabilities, but should also include regular modifications to it, thereby rendering an attacker's knowledge of the system obsolete.[104]

Cyber weapons, once discovered, can often be neutralized and their negative effects reversed.[105] Most importantly, as noted earlier, some believe that the ability to continually change network architecture, software, and processes is swinging the balance in the cyber realm in favor of the defense.[106] New technologies for intelligence collection and analysis may further help assign attribution and greatly improve a defender's ability to stop attacks. To constitute best practices, cyber defense must be in-depth, that is, based on multiple, overlapping, and mutually supportive measures designed to guard against a failure in any one technology or protection method. Defenders must also have clear command and control systems to assign responsibility for handling attacks as they happen.[107]

Defenses must be appropriate to the situation. In the initial stages of an attack, before systems have been penetrated or real damage has been caused, technological disruption may be adequate. Once this threshold has been crossed, however, defenses may have to focus on containment and in some cases on preventing the attacker from even knowing that the intrusion has been discovered and blocked. If successful, this would allow the defender to protect the system from further damage, learn how the attacker operates for future reference, and possibly even feed them misinformation.[108] A further defensive measure is to temporarily pull critical systems from the Internet, thereby isolating the threat and eliminating it.

Unlike conventional military threats, but much like other asymmetric ones, governments must work closely with private entities and the general public if truly robust cyber defense is to be achieved.[109] The effectiveness of governmental arrangements for sharing and disseminating cyber intelligence and information, both within the government and with the public and private sectors, is

critical. Public and private entities commonly recognize the need for such information sharing, but only relevant legislation can enable them to do so without fear of violating civil liberties and rights to privacy[110] as well as loss of commercial advantage.

Quandary 7: Should Hack Backs Be Allowed?

The right of a state actor to resort to countermeasures in response to a wrongful act is explicitly recognized in international law and presumably applies to the cyber realm as well.* In general, countermeasures are allowed only after the injured state has asked the other to cease or remedy the wrongful act, but exceptions can be made if urgent measures are necessary to preserve the injured state's rights and avoid further damage. Countermeasures can be taken against a state actor or persons or entities acting on its behalf, including private firms. Countermeasures must, however, be designed solely to induce the responsible actor to comply with its legal obligations or remedy the situation and, just as in the physical world, not be taken for purposes of retribution.[111]

If an attack was conducted against a governmental system, authorization for active defense would be governed by the specific state's cyber defense policies. These policies would have to establish clear guidelines regarding responses appropriate to the organization under attack, or type of organization, and be conducted in accordance with international law. The situation becomes far more complex, however, when private entities are the targets of the attacks, raising the question of whether, and under what circumstances, they should be authorized to conduct hack backs on their own recognizance.

The problem is particularly acute in regard to critical entities, such as power companies, hospitals, dams, or communications and banking systems, whose disruption can have immediate, disastrous, and even fatal consequences. An attack on a hospital might shut down life support equipment, an attack on a dam might lead to structural or operational failure, and an attack on a banking system could wipe out the wealth of a large part of a nation. When dealing with attacks such as these, the need for an immediate and even autonomous computerized response may render impractical a requirement that the private entity first consult with the relevant governmental authorities and gain their approval.

The Argument: Hack Backs Should Be Allowed—Conditionally—where governments cannot, or do not, provide public and private entities with

* The Tallin Manual 2.0 (see Chapter 9) states that "a state may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation."

sufficient defense against cyber attack, some believe that certain actors, such as IT or cyber security firms or even the entity attacked, should be authorized to conduct hack backs on their own. To avoid irresponsible behavior and even vigilantism, this authority would be limited to clearly defined and highly circumscribed circumstances and subject to stringent legal sanction.

In the physical world, for example, US law recognizes "certain rights of self-defense and the defense of property in preventing the commission of a crime against an individual or corporation." In some cases, the law provides for measures that go beyond passive self-defense, such as physically preventing an intruder from entering private property or pursuing the intruder beyond property lines. The United States further authorizes private security firms, bank guards, and university police forces to conduct a variety of law enforcement activities and even permits "bounty hunters" to conduct arrests. Numerous other states also authorize public and private entities to conduct a variety of law enforcement activities. The dangers of allowing hack backs are clear, but so are the costs of proscribing them. One can draw a relatively clear line between active defense that makes it more difficult for an intruder to steal data, such as honeypots and sinkholes, and offensive attacks on another's network.[112]

At least in certain circumstances, the public good may require that conditions be specified under which designated public and private entities are permitted to take active measures outside of their networks. The US Active Cyber Defense Task Force recommended that the government partner with the private sector to develop a framework for active defense, with strict governmental oversight, designed to enable forward-looking and technologically advanced private entities to defend their assets in the cyber realm. The Atlantic Council proposed a legal framework that would authorize certified private sector security providers to take limited active defense measures, under proper supervision of law enforcement agencies.[113]

The Counter Argument: No Way—Hack Backs Are Cyber Vigilantism—unsurprisingly, others take a more conservative approach. International law, they stress, makes no provision for a response to malicious cyber activity by a private entity, and only an injured state may take countermeasures.[114] The Commission on the Theft of American Intellectual Property worried that legalized hack back authority would be abused and recommended that only national security and law enforcement agencies have the legal authority to do so. It did, however, support adoption of cyber measures to identify stolen intellectual property and render it inoperable, such as marking electronic files with beacons and writing software that makes files inaccessible to unauthorized users.[115]

For the most part, private sector entities today may only respond to attacks within their networks, while states can act legally outside of them. For obvious reasons, few if any firms are willing to openly acknowledge that they engage in hack backs to regain information or destroy an adversary's system, but many do.

Indeed, a survey of IT practitioners found that fully 64% believed that their organizations either had already conducted hack backs or planned to do so. The banking industry appears to be particularly active in this field, but is far from alone. Some firms provide hack back services to corporate clients, at times going far beyond active defense to aggressive preemptive or retaliatory attacks. These firms often do not conduct the hack backs themselves but provide their clients with the expertise needed to disrupt traffic on the malicious actor's system and knock it offline, break into hard drives, find stolen property and delete or retrieve it, unleash a virus on an adversary's network, or delete everything on it.[116]

In 2009 Google concluded that Chinese hackers had obtained access to proprietary software it produced and provided US law enforcement and intelligence agencies with concrete evidence of the intrusion. Much as a property owner may follow a robber back to where he lives, Google did the same, tracking the intrusion to its source. Google was careful, however, not to remove, delete, or destroy any information on the targeted systems, which would have crossed a legal line.[117] In 2011 Facebook went further, taking control of a hacker group's server in order to exfiltrate evidence and disable it, but shared the information both with law enforcement agencies and the online security community. In 2013 Microsoft partnered with leading financial institutions, including Bank of America, American Express, and Chase, to disable a cluster of hijacked computers that were being used for online crime. Microsoft also took control of the servers used to conduct the attack, an act that would have clearly been illegal had the company not first obtained court approval and acted in conjunction with the FBI and law enforcement agencies in 80 countries.[118] In 2021, to disrupt a wave of attacks, Microsoft seized 42 websites used to collect intelligence by the state-backed Chinese hacking group Nickle, which had targeted foreign ministries, think tanks, and human rights organizations in 29 countries. Microsoft took care to carefully follow the law by taking this action only after it had received approval from a federal court in Virginia.[119]

These examples demonstrate that hack backs can be conducted responsibly and subject to appropriate legal sanction. The idea remains highly controversial, however, and opposition is widespread.

Quandary 8: Can Adversaries Be Defeated in the Cyber Realm?

Defeat in the physical realm has long been understood to refer to the use of force either to prevent an adversary from continuing to wage a conflict or undermine its psychological will to do so. To effectively defeat an adversary, certainly to

achieve decisive defeat, conquest and the occupation of territory have typically been required. Common public misperceptions to the contrary, decisive defeats, as in the "unconditional surrender" of World War 2, have actually been comparatively rare in symmetric and asymmetric conflicts alike.

Cyber conflicts, as noted, including offensive and defensive maneuvers, actually constitute attempts to gain or retain control over the confidentiality, integrity, and availability of information resources and the systems that process, transmit, and store it.[120] Although physical force is not used in purely cyber conflicts, it is in hybrid ones. Adversaries do not contest geographic territory, but they do contest "cyber terrain," defined as the other side's information resources, including the "high ground," that is, those resources that proffer a particular advantage to one or both sides. This terrain is constantly changing, and adversaries contest it by using the cyber equivalents of the traditional military concepts of reconnaissance, maneuver, and firepower.[121]

The Argument: Cyber Attacks Can Be Defeated—to achieve defeat in the sense that the adversary is no longer capable of waging conflict, states will have to be able both to defend the confidentiality, integrity, and availability of their own information resources and to successfully assert control over the adversary's. In the case of CNA attacks, this would entail gaining control over the availability and integrity of the information resources, in the case of CNE attacks, the confidentiality, and in the case of CNI attacks, the integrity.

US cyber strategy today is based not just on the aforementioned principle of "defending forward," to disrupt or halt malicious cyber activity, but explicitly on defeating adversaries and winning wars. Nevertheless, the means by which the strategy proposes to defeat adversaries in the cyber realm are very different from those in the physical world. Rather than decisive military defeat, which leads to an identifiable stage in which hostilities are terminated, US strategy views cyber defeat as the result of the aforementioned process of continuous engagement, designed to impose tactical friction and strategic costs on an adversary and in so doing compel it to shift resources from offense to defense.[122]

The UK cyber strategy, like the US, is based on offensive cyber operations designed to damage or disrupt an adversary's systems or networks. Unlike the US strategy, it is more conservative in its approach and does not define the adversary's defeat as the desired end state.[123]

The Counter Argument: Cyber Attacks Cannot Be Defeated—as in other areas of asymmetric conflict, including terrorism and insurgency, the very concept of defeat in the cyber realm is problematic. Physical force is not used, and geographic territory is not contested. Indeed, both state and nonstate actors can operate on systems that do not belong to them and nonstate actors can even operate without any cyber infrastructure or territory of their own at all.[124] The vast number of attacks possible and the highly diffuse nature of the threat probably

make decisive defeat of an enemy even more difficult in the cyber realm than in other areas of asymmetric conflict, particularly in terms of the psychological will to continue fighting.[125]

The ability to assert control over an adversary's information resources is a high bar and it will prove very difficult, in practice, to prevent an adversary from continuing to wage a conflict. Defeat of an adversary in the sense that it no longer has the psychological will to continue fighting would likely prove even more difficult to achieve. Further adding to the difficulty, most offensive effects on the availability and integrity of information are transient and, in the absence of physical destruction, the target may be able to restore operations within a comparatively short period of time. Offense is thus less decisive in the cyber realm than in the kinetic, making defeat of an adversary much harder to achieve.[126]

The Counter Counterargument: A Third Way—given what we have just discussed, we propose an alternative, two-tiered approach to the concept of defeat in the cyber realm. In practice, defeat at the first tier is likely to prove rare, as it has in other areas of asymmetric conflict, and the second is probably more realistic.

Cyber defeat—the ability to gain control over the confidentiality, integrity, or availability of an adversary's information resources to the extent that it is no longer capable of continuing to wage cyber conflict or no longer has the psychological will to do so.

Cyber superiority—the ability to impose a level of disruption or damage on an adversary that it cannot tolerate or at which it cannot function without significant dysfunction. Conversely, the ability to reduce the number and severity of adversary cyber attacks to a level that a state can tolerate and at which it can continue to function without significant disruption. If an adversary cannot successfully sustain attacks beyond this level, superiority has been achieved and it has, for all practical purposes, been defeated. Another way of defining superiority is the capability to deny the adversary the ability to achieve strategic objectives or, conversely, to achieve them ourselves.[127]

Clearly, the most straightforward path to achieving cyber superiority and even defeat would be to cripple an adversary's cyber capabilities. Given the highly diffuse nature of the threat, however, seeking to defeat all attacks and attackers will usually prove impractical. When dealing with adversaries with limited capabilities, defense will usually suffice. Conversely, when addressing threats from sophisticated actors, including major terrorist organizations, attacking their cyber capabilities may be necessary, whether by cyber or kinetic means. Sophisticated cyber attacks require extensive planning and expensive resources, in terms of personnel, equipment, technology, and intelligence, and thus create targets that the defender values. In so doing, they may provide the other state with the basis for deterring and, if necessary, achieving superiority over them.

In most cases, standalone cyber operations are unlikely to prove sufficiently effective to achieve defeat or superiority. To be truly effective, states will have to bring to bear the entire range of capabilities available to them, cyber, kinetic, diplomatic, economic, and otherwise, and to blend them into one coherent operational framework.[128] They may also have to pursue a process of "cumulative defeat," similar to the earlier concept of cumulative deterrence. In other words, cyber superiority or defeat is unlikely to be achieved in a single decisive round of hostilities, probably not even in a few. Rather, it is likely to be the outcome of a protracted process of continuous engagement, in which the adversary's attacks are repeatedly stymied and it ultimately comes to realize that its efforts are futile and that it no longer has the capability, or will, to persist. In effect, cyber superiority and defeat are a function of the state's ability to successfully combine all four D's—detection, deterrence, defense, and defeat—along with resilience. Cumulative strategies do not work quickly, however, and states can have difficulty sustaining them for extended periods, particularly democracies.

As in the physical world, the more significant the original disruption caused by a cyber attack, the greater the domestic and international legitimization for responding, especially by kinetic means. Public opinion, however, perceives cyber attacks to be less severe than kinetic ones, even when the actual damage caused is similar, and popular willingness to use kinetic force in response is thus more limited.[129] Decision makers will have to take this dynamic into account.

International cooperation is also of considerable importance in achieving cyber superiority or defeat, much as it may be in regard to detection, deterrence, and defense. It is easier to ascribe attribution and launch a counter offensive if other states help determine where an attack originated from and especially if they support or even participate in the effort to defeat it. Cooperation with foreign governments will further improve the ability of states to defeat adversaries by imposing sanctions and/or legal and criminal penalties.

Quandary 9: How Can Cyber Resilience Be Achieved?

Even the best defenses fail at times and some cyber attacks will get through and cause damage. The critical question then is how to recover as fully and as rapidly as possible and return to the antecedent state of functionality or thereabouts, that is, to build resilient systems.

The inherent limits on resources mean that it is essential to prioritize the systems to be made resilient. Different systems require different levels of resilience. Some only have to be able to return rapidly to some minimal level of

functionality, while others, such as power grids and sensitive military systems, must be designed to return to the original level fully and almost immediately.[130] The impact of the failure of a particular system on public morale is also an important factor to be considered. Attacks that undermine confidence in the ability of the government to provide basic public goods, satisfy needs, or protect the economy and citizen's private finances can be particularly damaging.

Features aimed at strengthening resilience can be built into network design to accelerate and support the recovery process. For the most critical networks, states can design cyber architecture that offers multiple pathways for controlling a particular system. This is more expensive, of course, but if one system fails, a backup exists. Resilient cyber systems also draw on a wide variety of technologies and policies designed to help defenders anticipate the timing and nature of attacks and address uncertainty.[131] To this end, intelligence regarding the adversary's intentions and capabilities (detection) can be vital in planning recovery from an attack.

Truly resilient systems and organizations must be able to work under degraded conditions in order to maintain at least some minimally defined level of functionality.[132] Resiliency can, however, only go so far, and eventually an attack will take down both a system and the response designed to deal with its failure. States can prepare for this eventuality and develop additional plans for living without a given system for more extended periods of time. This will likely require not just redundancy, such as ensuring that one is able to quickly move operations to a new network or set of computers, but also that options be developed that are not dependent on technology, for example, ensuring that train movements can be controlled manually.

Building resilience will also require that governments work closely with the private sector. In the United States, for example, roughly 85% of critical infrastructure facilities are owned and operated by private sector firms,[133] which are also responsible for facility maintenance, security, and operations. Government cooperation and regulation of the private sector is essential in order to ensure that proper resilience plans are in place, failures can be addressed effectively, and functionality restored as rapidly as possible.[134]

Hardware and software for both computers and smart phones are designed and manufactured around the world, raising questions of supply chain security. One way of addressing the potential dangers would be for governments to ensure that hardware and software for critical systems are not all acquired from a single source. A diversity of sources would allow states and firms to more quickly isolate a problem, switch to a different company's product, and resume normal operations. Another, more problematic approach, which some fear might have a deleterious impact on innovation, would be for governments to work in

conjunction with one another and with companies to develop an accreditation system for transparent and secure design and manufacturing processes.[135]

Quandary 10: How Has Cyber Changed State Power, Military Might, Warfare, and Statecraft?

We are left with one final, critical task in this chapter: trying to make some sense of it all. The cyber realm has undoubtedly had an impact on state power, military might, warfare, and statecraft. The question is whether it has been transformative or merely significant. This is a question that has been the subject of weighty tomes in its own right, and we will touch on some of the salient issues.

The Argument: Cyber Has Transformed State Power, Military Might, Warfare, and Statecraft—state power is a function of many factors, of which the ability to develop and deploy advanced civil and military cyber capabilities is an increasingly important one. In the civil area, a vibrant cyber ecosystem can be an important source of economic vitality and strength, but also a vulnerability, for example, through attacks against financial institutions, ransomware, or theft of intellectual property. Cyber information operations have become a critical means of sowing political and social discord, even havoc, and of disrupting political and governmental processes.

States that have successfully harnessed the advantages of the cyber realm for economic purposes have also been able to translate this into diplomatic influence and military power. Indeed, the traditional balance of global power is being upended and at least partially superseded by the competition for civil and military cyber power, in which both the United States and China seek dominance, and by gray zone cyber operations by China, Russia, and others. Competition for control of the technologies that underpin the future of the cyber realm, such as microchip production, cloud architecture, and mobile technology, are important critical components both of the trade war between the United States and China and of their national security strategies.[136]

The cyber realm and specifically cyber attacks are an increasingly important focus of international diplomatic discourse and contacts. In 2016 the United States accused Russia of ordering a sustained information attack on its presidential elections and in 2019 warned China of a technology war if it continued to conduct malign cyber activities. China, for its part, declared in 2015 that the cyber realm has become the new "commanding heights" of strategic competition and accused the United States in 2021 of being the "champion" of all cyber attacks. Cyber issues have largely come to replace the nuclear and arms control issues that were the focus of superpower summits in the past, including the

2021 meeting between presidents Biden and Putin. That same year, the Group of Seven intergovernmental political forum (G7) called on Russia and China to bring their cyber activities into line with international norms.[137] The list goes on.

Military cyber capabilities, as well as cyber espionage and information operations, now constitute major components of state power, supplementing and in some ways supplanting the classic sources. Military cyber power is a function of a state's ability to control information and the systems that process, transmit, and store it. Cyber conflicts, therefore, are contests for control over information resources. Future conflicts will be multidimensional, involving not just the traditional areas of warfare but also cyber attacks against civilians, civil sectors, and critical infrastructure as well as intense information warfare.[138] The United States believes that all significant military engagement in the future will include a cyber component and, along with China, envisages future warfare being won or lost in an AI (and space) augmented cyber realm.[139] Russia has developed an entire hybrid strategy of gray zone warfare, the Gerasimov Doctrine mentioned earlier. Some believe that the impact of cyber on the future of warfare will be no less dramatic than that of the Industrial Revolution and that it will require a fundamental rethinking of the nature of warfare.[140]

Much of cyber conflict takes place below the threshold of armed attack, without physical violence or conquest, but can still have severe effects. To mention just a few examples, Russia conducted the destructive NotPetya attack on Ukraine, which spread to 64 countries and 200,000 computer systems; a different cyber attack attributed to Russian hackers demonstrated the ability of cyber attacks to cause explosions and loss of life; North Korea paralyzed 230,000 computer systems in 100 different countries in the WannaCry attack; Iran shut down operations in Saudi Aramco in the Shamoon attack and disrupted 46 leading US financial institutions and later 200 major US and international firms; and China disrupted trains, the stock market, and hospitals in Mumbai.

Commercial and civil targets have always been a part of warfare, but in a world increasingly averse to physical and especially lethal damage, the cyber realm has demonstrated heretofore unprecedented capabilities to cause severe effects without harm to physical property or loss of life. Whether these attacks have actually caused changes in the targeted state's policies is certainly an important question, but not the critical one. Not all kinetic attacks force a change in state policy either, and a critical threshold must be crossed, in both kinetic and cyber attacks, before they may do so. The attackers in these cases certainly forced their adversaries to take their actions into account and achieved at least some modicum of deterrence.

Some cyber theorists and practitioners go beyond mere disruption and damage and believe that cyber attacks against critical economic, governmental,

and/or infrastructure networks may achieve systemic effects that severely undermine a state's socioeconomic vitality and basic ability to continue functioning. In so doing, cyber attacks would provide military victory without recourse to kinetic warfare and direct loss of life and lead to outcomes that no other military technology, conventional or unconventional, has ever achieved. Others are more skeptical and believe that while the capability to cause significant localized and temporary disruptions has already been demonstrated, the state of the literature is such that the ability to cause wide-ranging and sustained disruption is unclear.[141]

To date, devastating systemic effects such as these—attacks that can bring a country to its knees—have yet to be fully demonstrated, but they have been manifested in a more limited form in Russia's cyber attacks on Estonia, Georgia, and especially Ukraine. The United States, Russia, and China have already conducted intrusions into each other's power grids, in preparation for a future conflict. In the Olympic Games attacks (see Chapter 10), the United States planned to shut down Iran's economy at will. These and other attacks clearly showed that the capability to severely disrupt power, transportation, communications, financial and governmental systems, and in so doing, national life is no longer a feverish dream. Moreover, there is every reason to believe that even more disruptive and destructive attacks will prove feasible in the future. The socioeconomic, diplomatic, and military ramifications are clear and far reaching.

Cyber affects how and when militaries come into contact with one another. Unlike conventional conflicts, in which hostilities usually last for discrete periods of time, but very much like the asymmetric threats of terrorism and insurgency, cyber hostilities are ongoing and adversarial militaries are in a state of continual contact and friction.[142] The increasing interdependency of networks further means that a successful attack on one has the potential to cause even greater cascading damage by harming all systems connected to it, within a state and even internationally. Moreover, military infrastructure often comingles with civil infrastructure and numerous military systems, such as procurement, are closely linked to civilian ones. All weapons systems today have computer or electronic components that are vulnerable to disruption or destruction by cyber attack.

The debate in the literature over the asymmetric advantages proffered by the cyber realm has yielded conflicting conclusions. On the one hand, cyber has clearly been shown to provide otherwise weaker state and nonstate actors with deniable, under the radar, and asymmetric advantages with which to offset their adversaries greater power. To this end, they take advantage of advanced militaries' dependence on highly complex cyber technologies for command and control, navigation, targeting, procurement, and more, to create new vulnerabilities. Asymmetric strategies are not new and have been applied by the weaker side from time immemorial, but the cyber realm greatly amplifies them.

Iran and North Korea, which have repeatedly targeted the United States and other Western countries with cyber attacks, are prominent examples of this.

Other experts challenge the notion that cyber favors the weaker side and represents an asymmetric leveling of the battlefield. To the contrary, they argue that the advanced capabilities required to make effective use of the cyber realm actually strengthen technologically advanced states more than they empower weaker ones. Moreover, leading global powers, including the United States, China, and Russia, make use of some of the same asymmetric advantages that weaker actors, such as Iran and North Korea, use. Standalone cyber warfare, they aver, is unlikely to materialize, and it is only when combined with the concurrent or sequential use of kinetic force and other sources of state power, in which the leading powers' advantages are most pronounced, that cyber is likely to prove most effective.[143]

On a purely technological level, the contention that cyber has strengthened advanced states even more than weak ones may well be true. It is hard, however, to compare the incremental power that cyber has provided to the superpowers with the advantages that weaker states and terrorist organizations have derived from their cyber capabilities. Terrorist organizations use the Internet for operational planning, recruitment, training, fundraising, communications, espionage, propaganda, and information operations. Not as glitzy, perhaps, as the superpowers' cyber weapons are thought to be, but arguably a greater incremental addition to terrorists' capabilities than cyber has been to the conventional and unconventional capabilities of the superpowers.

It probably is not truly feasible to win wars by cyber means alone, and it is highly unlikely that major military confrontations in the future will be fought solely in the cyber realm. There is, however, little doubt that cyber provides the opportunity to achieve unique military objectives on its own, or that cyber measures can provide critical advantages when wielded in combination with other military capabilities. The United States has reportedly penetrated Chinese nuclear command and control systems, conducted cyber sabotage attacks against Iranian and North Korean missile programs, and planned on shutting down electricity in Syria at the height of the civil war, to ground its air force.

Cyber has had a major impact on the 4Ds. Detection of an adversary's intentions and capabilities is difficult in all types of conflict, and history is replete with examples of surprise attacks, both symmetric and asymmetric. Cyber, however, provides even greater possibilities for deception and plausible deniability, easing attempts both by state and nonstate actors to hide their actions and further increasing the danger of surprise. Advanced states' intelligence and technological capabilities today are such that attribution does not usually present an insurmountable obstacle, although not necessarily in a politically relevant time frame or at a level of demonstrable certainty.

The second D, deterrence is probably not feasible on its own in the cyber realm. To a greater degree than in kinetic conflicts, the ability to deter adversaries in the cyber realm is a function of a state's overall deterrent posture, based both on cross-domain and cumulative deterrence. States with a high level of cyber dependence will be particularly vulnerable to deterrence and even to the dangers of self-deterrence.

Cyber has had a particularly pronounced effect on the third D, defense. Cyber attacks circumvent the defenses provided by state borders, potentially upending the traditional role of national militaries as guardians of the state. The speed of cyber attacks and the ability to launch them concomitantly from essentially unlimited locations around the world have led to a consequent need for defenses that are equally rapid and increasingly automated, eliminating any possibility for deliberate responses by the national leadership. To a far greater extent than conventional conflicts, effective cyber defense requires that governments work closely with private entities and the general public, even raising the question whether private entities should be permitted to conduct some active defenses on their own.

Defeat of an adversary in the cyber realm, the fourth D, is particularly difficult to achieve, much as in other areas of asymmetric conflict. Unlike conventional warfare, but similar to counterterrorism and counterinsurgency, both cyber superiority and cyber defeat will usually stem from a process of continuous engagement, rather than a single or small number of decisive contests. Neither standalone cyber defeat nor superiority are likely to prove feasible, but when integrated into the entire range of capabilities available to a state and a coherent overall strategy, advanced cyber capabilities may proffer a decisive advantage and have a major impact on future warfare. The objectives, however, will remain much the same, that is, to deny an adversary the ability to continue prosecuting a conflict, impose a level of disruption or destruction that undermines its psychological will to do so, or reduce the number and severity of attacks to a level that the defending state can tolerate.

Espionage and information operations are further tools of statecraft. Neither are new, of course, but both have been changed dramatically, even revolutionized, by cyber. Cyber has become the primary means by which advanced states collect intelligence and conduct intelligence operations. The scale of modern-day cyber espionage simply dwarfs all previous capabilities. The NSA has implanted vast numbers of exploits in computers around the world and hoovers up untold quantities of data. It has reportedly penetrated China's national command and control systems, including for nuclear weapons. The Russian SolarWinds and Chinese Microsoft Exchange attacks demonstrated the massive, even global, reach of cyber espionage campaigns. Iran has conducted cyber espionage campaigns against US officials involved in the nuclear negotiations and the imposition of sanctions against it and has stolen sensitive information from

more than 1,800 employees of US aerospace firms. China's theft of intellectual property is of unprecedented scale and economic ramifications. China has also penetrated major US weapons development programs, the US legal system to uncover the names of potentially compromised spies, and a classified EU diplomatic cable channel. China, Russia, North Korea, and Iran use cyber means to surveille their domestic populations and suppress dissidents. China has even built a global surveillance capability for similar purposes.

States compete today over information and public perception, no less than in other areas. As with attacks designed for purposes of disruption and damage, or espionage, this competition does not necessarily take place on battlefields but on computers, smart phones, and the digital infrastructure that supports them. In practice, it takes place on three integrated dimensions: information (propagation, control, and manipulation); architecture (the systems and platforms that transmit and collect data); and governance (laws, norms, and standards for content, data, and technology). The ability of cyber means, especially social media, to reach huge numbers of people around the world, directly, instantly, and at minimal cost, has revolutionized information operations no less than the world of espionage. Long a staple of interstate rivalry, cyber has imbued information operations with vast new prospects, threatening the societal cohesion of states and their political systems.[144]

For democracies, the free and open flow of information, ideas, news, and political discourse is an empowering force in the hands of the people. This dependence, however, and the hands-off approach that democracies typically take toward the flow of information, provide authoritarian rivals with opportunities to intervene and to subvert their electoral processes, erode public confidence in the legitimacy of democratic institutions, sow political and social discord, and undermine the public's sense of socioeconomic well-being.[145] Russian interference in the US presidential elections between 2016 and 2020 demonstrated the disruptive potential that information operations can have and their ability to threaten the effective functioning and fundamental legitimacy of even the most deeply established electoral systems and governments.

For authoritarian states, the same free flow of information that is the lifeblood of democracies is a direct threat to their stability that must be controlled. States such as these, whether global powers like China and Russia or regional ones, such as Iran and North Korea, have thus sought to gain effective control over their domestic cyber realms and have succeeded in at least partially closing them off to outside influences and in using them as means of mass control and suppression. Nevertheless, their actions mask a deep fear of not just the cyber realm's potential impact on their domestic stability but also the legitimacy and longevity of their regimes. The Arab Spring was an early demonstration of cyber's ability to undermine and threaten the survival of authoritarian governments.

The Counter Argument: Cyber Has Not Had a Major or Transformative Impact on Military Might and the Nature of Warfare—some scholars question whether cyber attacks truly have the capability to cause serious damage to technologically advanced state actors. The cyber defenses of states such as these, they maintain, are robust enough to defend against attacks and the most critical systems, such as sensitive military ones, are not connected to the Internet in any event. The vulnerability of states to cyber attacks is further limited, as is the utility of cyber attacks for purposes of warfare, because the damage caused can usually be repaired comparatively quickly.[146]

Two more fundamental contentions have been raised. First, some assert that cyber attacks are making state interactions less violent than they were in the past and that cyber war will not take place. All cyber attacks, according to this line of reasoning, are essentially just more sophisticated but less violent versions of three activities that are as old as human conflict: sabotage, espionage, and subversion. Cyber sabotage enables highly targeted attacks against enemy capabilities without putting either the attackers or defenders at risk. Cyber espionage makes it possible to exfiltrate large quantities of data without endangering the lives of agents. Cyber subversion enables mass mobilization of followers for political causes, including threats to the legitimacy and stability of regimes, with less need for direct forceful action by activists. War, however, these theorists maintain, is violent by definition and is used as a means of compelling an adversary to accede to one's demands. An action that is not at least potentially violent does not, therefore, constitute an act of war. Computer code does not have its own force or energy and thus cyber attacks cannot constitute acts of violence and war. Cyber attacks may have violent consequences, but they are indirect.[147]

The second contention is that most activities in the cyber realm have little to do with the use of force or fall well below the threshold of armed conflict. As such, they may be better conceived of as intelligence contests, rather than military confrontations. An intelligence contest such as this includes competition in five areas: collection of more and better information; exploitation of the information to improve one's relative position; reciprocal efforts to covertly undermine the other side's morale, institutions, and alliances; attempts to disable adversary capabilities through sabotage; and pre-positioning of assets for intelligence collection in the event of future conflict. In intelligence contests, far more than in military conflicts, it is difficult to assess the balance of capabilities and achievements and who is "winning" at any given time, at least partly because the contestants operate in secret.[148] Since intelligence contests are waged by entirely unequal actors, for example, the United States versus North Korea or Iran, they can be considered a form of asymmetric conflict, along with terrorism and insurgency.

These are important arguments, but they suffer from a number of weaknesses. First, there is a definitional issue. Some of the scholars who question the actual impact of cyber on the nature of warfare and international relations generally define damage solely in physical terms, excluding harm to various capabilities, economic costs, and even reputational damage.[149] This is an overly restrictive definition that does not account for the changes wrought by the cyber realm, and, in any event, cyber attacks are increasingly capable of causing severe physical damage.

Moreover, events have largely overtaken these arguments. The cyber defenses of technologically advanced states may be robust, but attacks have successfully penetrated crucial civil systems and even sensitive military ones. In numerous cases, it has not, in fact, proven easy to root out intrusions and to stop attacks and many remain ongoing, such as Russian, Chinese, and US penetrations of each other's power grids. In some cases, recovery from attacks can take days, or even weeks or months, which are usually intolerable periods of time. Cyber interactions themselves may be less violent, but they are increasingly capable of severe second or third order physical damage and even lethal effects.

Furthermore, the skeptics refer to standalone cyber warfare and to protracted conflicts between state actors, neither of which are probably realistic scenarios in the international system today, as a whole, and certainly in the Middle Eastern context. While some effects of cyber attacks can be remediated rapidly, even temporary disruptions of critical systems can have severe ramifications. This is especially true in conflicts that last just days or weeks, as is true of most conflicts that Israel and increasingly other states are likely to be involved in, where disruptions lasting just minutes, certainly hours, could have a critical impact.

Finally, the overlap between military and intelligence contests is far greater than has been suggested, to the point that it is hard to differentiate between an ambitious intelligence contest and low-intensity or asymmetric military conflict. This approach is helpful, however, in that it provides a further indication of cyber's character as a manifestation of asymmetric conflict.

State behavior to date does not provide clear answers to the theoretical debates over such issues as the relatively escalatory or non-escalatory nature of the cyber realm compared to the physical world, although the evidence appears to lean to the latter. There have only been three known cases to date of kinetic responses to cyber attacks, and leading state actors, such as the United States, have often refrained from escalating even on a cyber level. In some cases, the damage has not been deemed worth the cost of further conflict, in others, countervailing political, economic, or other considerations outweighed the retaliatory incentives, that is, the target was deterred from responding. NATO, for example, was unwilling to respond to clear Russian aggression in Estonia, Georgia, and Ukraine. The United States wished to avoid escalation despite massive Chinese theft of

US intellectual property and North Korea's attack on Sony. It also remains unclear whether cyber is offense or defense-dominant and the balance is continually evolving.

Although the cyber realm has produced dramatic changes in the nature of state power, military might, and statecraft, it has not changed the fundamental nature of warfare. States still engage in offense and defense, cyber versions of the classic reconnaissance, maneuver, and firepower, and states still contest "cyber terrain." The 4Ds still generally apply to the cyber realm, even if they are manifested differently in some ways from the conventional and nonconventional realms. To say that there are important areas of continuity does not detract from the magnitude of the change cyber has caused in the sources of state and military power and in the nature of warfare. In all areas it has been significant and in some truly transformative. This is more than enough to justify the interest in the field.

PART II

WAR BY OTHER MEANS

The Cyber Threat to Israel

Starting in the late 1990s, the cyber realm posed a new addition to the array of threats that Israel had long faced. As such, we posited in the Introduction that Israel's initial response to the cyber realm was a matter of strategic necessity, as would be predicted by the realist school of international relations theory.

Part II presents the cyber threat to Israel. Chapter 4 provides a general overview of the threat and a detailed account of the primary attacks that have taken place to date. Given Iran's overarching strategic importance for Israel, Chapter 5 is devoted solely to its cyber strategy and institutions and to the primary attacks that it has conducted to date against both Israel and other primary targets. In essence, Chapters 4 and 5 constitute the realist independent variable regarding the strategic imperative behind the development of Israel's cyber capabilities.

4

The Overall Cyber Threat to Israel

Flee for your lives and get out of our country . . . wait for our pressure, the pressure will be fierce.

Hamas hack of Israeli TV channel

They have forcibly stripped us . . . none of our encrypted systems are probably safe from them. This is the worst leak in the history of Israeli intelligence.

Senior Israeli defense official describing a US-UK cyber-intelligence operation

Israel is a highly cyber-dependent state. The potentially severe array of civil and military cyber threats it faces have joined and, in some ways even superseded, a long list of existing conventional and non-conventional threats. Indeed, former Prime Minister Netanyahu even stated that the cyber realm constitutes one of the four primary threats that Israel faces. This concern is clearly reflected in the IDF's official strategy statements.[1]

Chapter 4 has three sections. It begins with a general overview of the cyber threat to Israel. The second section presents the primary cyber attacks conducted against Israel to date by state actors, other than Iran, which is addressed in the following chapter. The third section presents the primary cyber attacks conducted against Israel by nonstate actors.

The Cyber Threat to Israel—A General Overview

Israel faces a nearly constant barrage of cyber attacks from state and nonstate actors alike,[2] ranging widely in terms of the types of targets chosen, extent of damage intended, and level of sophistication. Attackers have targeted virtually every possible network in Israel, during times of both peace and conflict and including military and governmental systems, hospitals, universities, financial institutions, and a variety of private firms.[3] Thirty-five percent of all cyber attacks against Israel in 2016–2017 targeted government agencies, 25% were against

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0005

technology companies, and 10% were against the financial sector.[4] In 2019 alone, 68% of private firms in Israel experienced some form of cyber attack,[5] while 2020–2021 saw a dramatic increase in the overall number of attacks that was twice as high as the global average, especially ransomware attacks.[6]

Israel's critical national infrastructure has been the focus of repeated attacks. In 2014 a large-scale attack was launched against the communications system,[7] possibly the earliest report of an attack against critical infrastructure. The Israel Electric Corporation (IEC), the primary provider of electric power to the nation, faces numerous cyber attacks every day, hundreds of thousands if one includes simple and easily deflected ones, but also sophisticated attacks specially tailored to penetrate and disable the entire system.[8] A successful strike on the electric grid could disrupt power to virtually all of Israel and simply shut the country down, with severe civil and military consequences. In 2016 an IEC employee fell victim to a spear phishing attack and unwittingly downloaded malware onto its computer systems, necessitating a temporary shutdown of the company's computers and parts of the electric grid.[9] That same year, an attack on the regulatory agency responsible for oversight of the IEC, the Israel Electric Authority, required a temporary shutdown of some of its computers.[10]

A successful attack on the communication system could cause havoc; a successful attack on the Israel Water Authority could cut off the national water supply. In 2020 a number of attacks took place against water facilities, possibly with the intent to poison the supply.[11] To date, none of the attacks against Israel's critical infrastructure have achieved effects of national magnitude, but not for lack of intent or trying.

As noted in the Introduction, hackers almost succeeded in disrupting the televised broadcast of the Eurovision Song Contest held in Israel in 2019, which is viewed live by hundreds of millions of people around the world, by inserting fake video of rockets raining on Tel Aviv.[12] In 2020 hackers attacked Ben-Gurion airport and incoming flights to Israel, in the attempt to disrupt the arrival of tens of world leaders attending a commemoration of the 75th anniversary of the liberation of Auschwitz.[13] The damage to Israel's international image, had either of these attacks succeeded, would have been severe. Another attack in 2020 targeted Israeli research centers working on a coronavirus vaccine.[14] The #OpJerusalem campaign that year attacked over 100 Israeli websites, taking advantage of a vulnerability in a web browser add-on used by thousands of sites in Israel.[15]

Much like the United States and other democracies today, Israel is concerned about attempts to subvert its electoral processes and influence public opinion through cyber means, including manipulation of social media and Internet sites.[16] Since voting in Israel is done with paper ballots, the actual vote count is not susceptible to cyber subversion, but websites belonging to the political parties and the Central Electoral Committee are. There is also considerable

concern that foreign actors, chiefly Russia and Iran, may conduct cyber information campaigns in the attempt to further inflame the nation's domestic divides, sow discord and perhaps undermine the legitimacy of the democratic system, or affect electoral outcomes.[17] Indeed, foreign actors posted 10,000 messages on social media prior to and during the April 2019 elections.[18] In 2020 Iran sought to amplify Israel's domestic tensions, to weaken it from within, and has waged ongoing information operations against it.[19]

Israel relies on a largely reservist army, with exceedingly short mobilization times. A cyber attack that disrupted transportation systems even for a short period, something as basic as shutting off traffic lights, could disrupt the mobilization of forces and have a significant impact on the conduct of military operations. Each year, the IDF faces hundreds of attempts to break through its defenses and penetrate military computer systems and networks, including operational ones.[20] Indeed, 10% of all failures in IDF computer systems in 2016, including operational and classified ones, were reportedly the result of cyber attacks, or suspected ones.[21]

A successful attack on sensitive military networks could present severe dangers, potentially crippling critical military capabilities. A source of particular concern is that the IDF's primary weapon systems are built in foreign states—aircraft, for example, in the United States, submarines and surface vessels in Germany—meaning that they may be infected with malware during the manufacturing process and that the IDF must conduct decontamination efforts following delivery.[22] Another source of particular concern is that a cyber attack could escalate and lead to a kinetic military confrontation.[23]

The intensity of cyber attacks against Israel has been shown to increase significantly during periods of heightened military tensions and even major diplomatic activity, such as the US recognition of Jerusalem as Israel's capital.[24] During the major rounds of conflict with Hamas in recent years, in 2009, 2012, and 2014, Israel faced particularly intense periods of cyber attack. Attackers were able to deface or block access to dozens of websites of government agencies, banks and financial institutions, and hospitals, as well as private websites and email accounts.[25] Traffic to and from Israeli Internet providers was frequently redirected and some Israeli users could not access foreign IP addresses.[26]

During the 2009 conflict Israel was hit with four waves of progressively stronger cyber attacks. At the height of the operation, government sites received 15 million junk mail deliveries per second from at least half a million computers. Among those taken offline were the public websites of the Israel security agency (ISA, known as Shin Bet or Shabak) and the Home Front Command, which instructs the public on means of protecting itself from rockets and other threats. During the 2012 conflict over 100 million cyber attacks were launched against Israel and roughly 2,500 mostly governmental websites were defaced, including

the offices of the president and prime minister and the Foreign and Defense Ministries. As in 2009, the websites of both the Bank of Jerusalem and El Al were taken down, the IDF's public site was disrupted, a major Israeli Internet provider's services were heavily slowed, and attackers posted passwords for thousands of Israeli websites.[27] During the 2014 conflict Hamas attacks were the most massive in number and sophistication. The overall number of attacks was smaller in 2021, presumably because Israel had destroyed most of Hamas's cyber capabilities the year before and at the beginning of the fighting (see Chapter 10). Nevertheless, Twitter accounts linked to Iran disseminated anti-Semitic messages at a rate of 170 times per minute, including "Hitler was right" and "kill all Jews."[28]

As with other countries, cyber attacks can pose problems of attribution for Israel. In each of the above confrontations with Hamas, for example, the waves of attacks against Israel apparently originated from somewhere in the former USSR, possibly paid for by Hamas or Hezbollah and abetted, or conducted, by Iran. Other attacks appear to have originated in such disparate states as Egypt, Morocco, Algeria, Turkey, Russia, Ukraine, Romania, the United States, France, Germany, Canada, Holland, China, Indonesia, Vietnam, and Singapore.[29] A DDoS attack of unknown provenance in 2021 led to a crash of the website of the National Insurance Institute (social security).[30] In the absence of proof at the level required for a court of law, attribution of these attacks is an analytical conclusion, presumably sufficient for intelligence and policymaking purposes and made easier by the limited number of adversaries that Israel faces. Nevertheless, the difficulties encountered in attributing such attacks illustrates the usefulness of proxies in the cyber realm, as in other areas of asymmetric conflict, including the ability to act covertly and maintain plausible deniability.

Cyber attacks against Israel also raise interesting issues regarding the attackers' political motivations. Many of the attacks have been conducted without any specific political agenda or set of demands and have been offshoots of wider campaigns aimed at undermining Israel's international standing, weakening it economically, and undermining its societal resilience and resolve. While a limited number of cyber attacks are unlikely to compel Israel to change its policies, the constant bombardment is designed to disrupt daily life and governmental functions, wear Israel down, and ultimately force changes in policy.[31]

Although not a focus of study in this book, dangers to Israel's cyber realm also stem, of course, from domestic sources. Israel's entire Population Registry was stolen by an employee of the Ministry of the Interior and illegally distributed in 2006, enabling cross referencing of the information with other available data sets and providing numerous opportunities for use by malicious actors. Voter data legally provided to the political parties as part of electoral campaigns has been treated in a cavalier fashion. A vulnerability in an app used by Likud in the March 2020 elections led to a leak of the personal data of nearly 6.5 million

people, including names, addresses, ID numbers, and more.[32] A flaw in an IDF Covid app, on which soldiers were required to report their health status during the Covid-19 pandemic, would have enabled any adversary to obtain the entire list of IDF soldiers, including their ID numbers and health status.[33]

Cyber Attacks by State Actors

The publicly available information on cyber attacks conducted against Israel by state actors, other than Iran, is limited. Whether this reflects the actual level of attacks against Israel, or the limitations of the information, is unknowable. The latter is more likely.

Russia and **China** are a source of particular concern for Israel, including reports of possible attempts by the former to interfere in Israel's electoral processes and claims that both have succeeded in penetrating important Israeli networks, such as critical national infrastructure, far more deeply than previously known. Indeed, concern in Israel grew so great that the National Security Staff was charged with drafting a special report on the topic in 2019.[34]

Russian trolls, operating out of the infamous Internet Research Agency in St. Petersburg, are reported to have used social media in attempting to influence and disrupt the US-Israeli relationship.[35] Other attacks are also known to have been launched from within Russia,[36] but whether the Russian government was complicit cannot be confirmed. A small number of Israeli firms and government agencies were among the approximately 18,000 clients worldwide who downloaded the malware in the devastating Russian SolarWinds attack in 2020, which focused primarily on US entities (see Chapter 2).[37]

Some consider Russia a bigger threat to Israel in the cyber realm than China, because of its greater involvement in the Middle East and the danger of Moscow passing sensitive information to states that are hostile to Israel and even of actively collaborating with them, as Russia reportedly already does with Iran.[38] The relative danger posed by the two countries may now be changing, however.

A well-informed source believes that China's efforts to promote its national economic and technological objectives by means of cyber espionage around the world are likely mirrored in Israel, as well. China's primary focus of attention is presumed to be the defense establishment, including the IDF, defense industries, and private firms that work for them, especially given their close ties to the United States, China's preeminent adversary. Major weapons systems developed in Israel, in some cases in cooperation with the United States or by Israeli firms with US subsidiaries, and Israeli-made components of US weapon systems, are thought to be of particular interest. Israeli academia may also be of interest, given its extensive ties with the security establishment.[39]

China's involvement in the Middle East was traditionally limited to the economic realm, and Israel tended to view it more as a commercial opportunity than a national security and cyber threat. Under US pressure to change its policies toward China, as well as the impact of a major strategic cooperation agreement signed by China and Iran in 2021, this Israeli perception has begun changing, but the context is important. As part of its drive for global commercial leadership, China has procured or stolen advanced US technologies, including AI, robotics, autonomous vehicles, and virtual reality, but has been increasingly prevented from doing so by the United States on national security grounds.[40] This failure presumably contributed to China's rapidly growing interest in Israel's high-tech sector and consequently to heightened US concern regarding Israeli sales of advanced technologies. In 2019, following three years of heavy US pressure to establish an oversight mechanism for "foreign," that is, Chinese, investment in its infrastructure and high tech firms, especially cyber ones, Israel began taking measures to do so.[41]

In practice, little is publicly known regarding Chinese cyber attacks against Israel. In 2011 and 2012 China reportedly conducted cyber espionage attacks against Israeli defense companies. Hackers affiliated with the People's Liberation Army, called the Comment Crew, allegedly stole blueprints for the Iron Dome and Arrow rocket and missile defense systems, as well as ballistic missiles and UAVs, from three Israeli defense firms.[42] Israel Aircraft Industries, one of the three firms allegedly attacked, denied the reports, claiming that they had been conflated with an attempt to penetrate its non-classified network.[43]

In 2013 Chinese-sourced malware was discovered on the computers of 140 senior Israeli security and defense industry officials.[44] In 2019 an Israeli infrastructure firm, which was competing with a Chinese rival for a tender to build a desalination plant, was hacked. There is no proof that the attack was conducted by China, or any other state actor, but it was considered particularly sensitive because of the future plant's location, adjacent to the Palmachim Air Force base and Sorek nuclear facility.[45]

The only major Chinese cyber attack against Israel known to date was a two-year-long espionage operation during 2019–2020, in which the hackers masqueraded as Iranians. The attack targeted tens of governmental bodies, defense agencies, academic institutions, and high-tech firms, possibly to gain business intelligence regarding the negotiations over multibillion-dollar civil infrastructure projects that Chinese companies were competing for at the time in Israel. To reduce the chances of discovery, the hackers conducted the initial intrusions on Saturdays, when businesses in Israel are closed, but exfiltrated information on weekdays, so that the data transfer would not stand out as unusual. The attempted deception demonstrates the importance of accurate attribution for Israel, as for all other actors.[46] In 2021, tens of private and governmental

bodies in Israel were again subject to a cyber attack, likely Chinese, for purposes of technological, business, and industrial espionage.[47]

In 2020 the **North Korean** Lazarus Group, thought to have played a role in both the 2014 attack on Sony and the devastating 2017 WannaCry ransomware attack (see Chapter 2), targeted Israel's defense industry. Although Israel claimed that the hackers were deflected and that no harm had been caused, outside experts maintained that it successfully penetrated the targeted computer systems and stole large quantities of classified data that might end up in Iranian hands.

The attack began with a LinkedIn message, in which the North Korean hackers, posing as Boeing headhunters, reached out to a senior engineer at an Israeli defense firm and to other targets. The Boeing employee was a real person, one of a number of headhunters from prominent defense firms whose LinkedIn profiles the hackers had cloned. At a certain point, the targets were asked to send a list of their job requirements in a file that was actually designed to penetrate the classified defense networks they were part of. The attack in 2020 was considerably more sophisticated than attempts in broken Hebrew the previous year, likely the result of an electronic translation, which immediately aroused suspicion.[48] The Lazarus Group has reportedly also conducted dozens of attacks against Israeli crypto exchanges, making off with tens of millions of dollars.[49]

Cyber attacks against Israel have reportedly also been launched from **France**, **Germany**, **Canada**, **Holland**, **Romania**, **Ukraine**, **Vietnam**, and **Singapore**.[50] Surprisingly, there is almost no information regarding cyber attacks launched by Arab states against Israel, although some may have been launched from their territory, including phishing attacks from **Morocco**, **Algeria**, and **Tunisia**.[51] Why this is the case is not clear, but it may reflect Israel's growing military ties in recent years with Egypt, Jordan, and the Gulf states, a general lack of capability, or in the case of Syria, the Arab state with the greatest motivation to attack Israel, an overwhelming preoccupation with its devastating civil war.

Ironically, allies such as the **United States** and **UK**, may have posed some of the greatest threats to Israeli cyber security. In 2008 both reportedly spied on Israeli drone and missile defense tests[52] and released information regarding Israel's use of attack drones, which it had not publicly acknowledged up to that time.[53] For a period of some 18 months in the mid-2010s they are also said to have hacked encrypted transmissions from IDF planes and drones in order to monitor Israel's operations in Gaza and the West Bank, as well as possible preparations for an Israeli airstrike on Iran's nuclear program.[54] A senior Israeli defense official described the US-UK attack as "an earthquake" and stated that "it means that they have forcibly stripped us and, no less importantly, that none of our encrypted systems are probably safe from them. This is the worst leak in the history of Israeli intelligence."[55]

Cyber Attacks by Nonstate Actors

For nonstate actors, the cyber realm is a further means of countering Israel's conventional superiority and of wreaking havoc,[56] especially during times of military conflict. Most of the information available, by far, is in regard to Hamas, much less so Hezbollah and other organizations. In practice, Hezbollah is thought to have the most advanced cyber capabilities of the nonstate actors Israel faces.

Hamas—most Hamas cyber attacks have been conducted for purposes of espionage and, secondarily, damage. Its cyber information campaigns have been more limited.

CNA attacks—in 2012 Hamas announced that it had begun a new type of "resistance" against Israel, this time in the cyber realm. A group of pro-Palestinian hackers, called Nightmare, for which Hamas took credit, briefly brought down the websites of the Tel Aviv Stock Exchange and El Al Airlines and disrupted activity on the website of a major bank.[57]

Hamas's cyber attacks against Israel during the 2014 conflict in Gaza were considerably more sophisticated than during the 2009 and 2012 rounds. Many of the sites targeted were now better defended and thus more difficult to attack, demonstrating the steady improvement that had taken place in Hamas' capabilities, possibly with Iranian assistance. Most of the attacks targeted Israel's civil infrastructure, financial systems, and governmental and military networks, including an attempt to seize control of IDF drones. The Home Front Command's website was repeatedly taken off-line, as was the Tel Aviv Police Department's website.[58] Attacks such as these can result in a loss of life, if the public does not get essential information, and can be demoralizing, when the adversary succeeds in disrupting wartime services.

In 2018 Hamas tried to hack the IDF Central Command's warning system against terror attacks in the West Bank. Had it gained control of the system, Hamas would have also been able to thwart essential IDF defensive capabilities.[59]

CNE attacks—between 2012 and 2019 and maybe since, the Hamas-affiliated Gaza Cybergang Group (aka Desert Falcons, Molerats, and SneakyPastes) repeatedly targeted government offices, defense industries, embassies, journalists, banks, and financial institutions in Israel, the West Bank, Jordan, Lebanon, Egypt, and the United States, once again with possible Iranian assistance. In 2017–2018 the group sent emails from ostensibly legitimate sources in an attempt to trick targets into installing malware.[60]

In 2015 Gaza-based hackers, presumably Hamas affiliated, used a pornographic video clip to lure Israeli targets into opening an email link, which then downloaded malware onto their systems. Disguised to look like Skype-related files and to have originated from IP addresses in Germany, the malware searched

for information of interest and relayed it back to the hackers. The attacks targeted an Israeli government office, IDF unit, transportation firm, and academic institution. The targets' reluctance to acknowledge having viewed inappropriate material at work and consequent hesitance to report the incidents lengthened the period of time until the malware was discovered and blocked.[61]

Starting in 2016 Hamas attacks at least partly changed course, possibly with Hezbollah's help. Instead of attacks against comparatively well-defended Israeli computer systems, Hamas began focusing on individual IDF soldiers,[62] making use of a variety of social media apps. Posing as attractive Israeli women or fellow soldiers, Hamas hackers encouraged the targets to download a video chatting app, actually a Trojan horse that gave them control over the soldiers' phones and enabled them to access their contacts, emails, conversations, videos, photos, and GPS locations, information of potentially considerable importance during times of military conflict. Even more importantly, it allowed them to remotely activate the phones' cameras and microphones, listen to the soldiers' conversations and film their surroundings, including military bases and formations.[63] In some cases, they were presumably even able to hear operational briefings and a variety of formal and informal exchanges.

A more concerted and sophisticated effort began in 2017, when Hamas started using fake dating sites to entice soldiers into downloading malware and later took advantage of the buzz around the 2018 soccer World Cup to further lead them on. A special World Cup app (Golden Cup) successfully bypassed Google's testing systems and was offered for free in the Google app store. Once installed, the app activated the malware. Hamas further augmented its efforts by creating fake Facebook profiles, again of attractive young women, which they used to establish relationships with the soldiers over a period of more than a year, indicating the seriousness of the effort and the degree of planning required. Only after the hackers had successfully gained the soldiers' confidence did they suggest that they download the dating apps and later Golden Cup.

In 2018 Hamas began using Instagram for similar purposes, to gain control over soldiers' phone cameras and audio recorders. Fitness apps were also used to access the phones of soldiers jogging near the Gaza border, where fighting was taking place. In all, over 100 soldiers, possibly hundreds, were duped into downloading the dating and soccer sites at a time of heightened tension and fighting, including ongoing rocket and other attacks. The soldiers' suspicions were aroused eventually, and they turned to the relevant IDF authorities.[64]

During the round of fighting in 2018, Hamas tried to hack Israeli phone users generally, using a fake version of a real rocket alert app, which provides precise real-time warnings. In 2019 Hamas hackers posed as IDF paratroopers, an elite and highly respected unit, and made use of actual classified IDF information to

turn to soldiers on WhatsApp to try to trick them into divulging secrets about their training and operational schedules.[65]

In 2020 Hamas attackers demonstrated a further improvement in their skills, posting more fully fleshed-out social media profiles of attractive women on Facebook, WhatsApp, Instagram, and, for the first time, Telegram. To avoid the need to communicate by voice, after the targeted soldiers had downloaded the malware, the decoy profiles claimed to be hearing-impaired or to have speech impediments and to allay any suspicions regarding their poor command of Hebrew, they further claimed to be new immigrants to Israel. In other cases, Hamas used short recordings of female Israeli voices. The smart phones of hundreds of officers and soldiers were targeted, and the attack was only discovered when Hamas reused a fake identity from a previous attack.[66]

By 2022 Hamas had significantly further improved its capabilities. Hackers used social engineering techniques to find their targets and lure them, as well as fake Facebook profiles to trick soldiers and police officers into downloading malware which provided them with control over their phones and computers. The fake accounts were set up months in advance, extremely active and well-versed in Israeli politics and current events. Unlike the past, they chatted with their targets in perfect Hebrew, typically engaging in a discussion around sexual themes. After gaining the target's trust, the hackers would then suggest that they move to WhatsApp, thereby gaining the target's mobile number. In some cases, they also suggested using a supposedly safer and more discrete means of communication, a fake messaging app called "Wink Wink Chat." Victims were specifically targeted during working hours, in the hopes of infecting their work computers.[67]

A potentially more sensitive Hamas cyber operation took place in 2018, following a highly classified and badly botched Israeli intelligence operation in Gaza. Posing as prominent Israelis, including then Prime Minister Netanyahu and former Foreign Minister Tzipi Livni, Hamas posted pictures on Twitter and Facebook of the commandos who had supposedly participated in the raid. The pictures were designed to coax Israeli users into commenting on and in so doing divulging further information about what had happened. In a highly unusual move, the IDF turned to the public and asked that it not respond in any way, because even information that seemed entirely innocuous might abet Hamas's intelligence gathering purposes and help it gain an understanding of the nature and objectives of the operation.[68]

In 2020, immediately following the peace agreement between Israel and the United Arab Emirates (UAE), the Gaza-based hackers launched a series of cyber attacks against senior officials in the UAE, Egypt, and Saudi Arabia, in order to gain information about their relations with Israel. The attackers set up fictitious profiles on Facebook, in which they posted information dealing with current

affairs, as a means of enticing the officials into downloading malware. The same hackers have repeatedly conducted attacks against the Palestinian Authority, as well, reaching a new level of sophistication in 2020.[69]

Ever since 2018, Hamas has operated a secret cyber headquarters in Turkey, from which it has conducted cyber attacks and counterintelligence operations against Israel, as well as the Palestinian Authority, Saudi Arabia, and the UAE. The headquarters was established without the knowledge of Turkey's government and operates independently of Hamas's official offices there.[70]

CNI attacks—in 2016 a popular reality show on Israel's Channel 2 was disrupted by anti-Israel messages followed by images of rocket attacks. "Flee for your lives and get out of our country" the Hamas message warned in Hebrew and Arabic. "You murder women and schoolgirls in cold blood . . . So wait for our pressure, the pressure will be fierce." The disruption lasted for over three and a half minutes and was displayed against a backdrop of past terror attacks, including gruesome video footage of an attack in Tel Aviv and images of the bodies of victims and funerals for fallen soldiers.[71] Later in 2016 two Israeli television news programs were briefly replaced by images promoting Islam, a message suggesting that a recent spate of fires in Israel had been divine retribution, and a Muslim call to prayer.[72] In 2017 a massive CNI attack, designed to take over Israeli television and radio broadcasts and induce public panic, was thwarted by the ISA.[73]

Hezbollah—Iran established Hezbollah in the early 1980s as a proxy in Lebanon, both to strengthen the local Shiite community and as a forward base of operations for the conflict with Israel. In the ensuing decades, Iran has provided Hezbollah with a mammoth rocket arsenal and advanced anti-aircraft, drone, and electronic warfare capabilities, among others, and it is hard to imagine that it has not done so with cyber, as well. As in other areas, the limitations of the publicly available information are thus presumably a function of Hezbollah's effective attempts to maintain operational secrecy.

Hezbollah reportedly conducts 10-day training camps in Lebanon in which thousands of Iranian-backed social media activists are taught how to conduct propaganda and disinformation campaigns. Designed to create "electronic armies" across the region, trainees from countries such as Iraq, Saudi Arabia, Bahrain, and Syria are taught to digitally manipulate photographs, manage large numbers of fake social media accounts, make videos, and avoid the censorship techniques employed by social media firms.[74]

In 2021 the IRGC's Quds Force helped Hezbollah establish a new cyber unit to counter espionage and subversive activity against it and Iran, under the command of Hezbollah leader Hassan Nasrallah's son. Possibly a response to Iran's growing sense of vulnerability, following the US assassination of Quds Force Commander Qassem Soleimani in 2019 and Israel's reported assassination of

the head of Iran's nuclear program the following year, the new unit reportedly attacks Lebanese cellular communications, social networks, and government agencies to collect information.[75]

CNA attacks—a sophisticated, multi-year Hezbollah attack, designed to circumvent the built-in protection systems in IDF computers by targeting the firms that supply software for them, was discovered in 2015.[76] Beyond this, there is essentially no publicly available information on CNA attacks by Hezbollah.

CNE attacks—in 2010, in what may have become a model for Hamas, Hezbollah hackers created a fake Facebook persona showing an attractive young woman lying on a sofa and smiling. Approximately 200 IDF soldiers responded to her friendship requests, subsequently providing information about the names of other service personnel, detailed descriptions of bases, and even codes. Nearly a year went by before the ruse was uncovered.[77]

In 2012 Hezbollah conducted a cyber espionage program, possibly with Iranian involvement, dubbed Volatile Cedar. Using custom built malware, the campaign targeted military suppliers, telecommunications firms, media outlets, and universities in Israel and approximately a dozen other countries.[78] In 2015 Hezbollah hackers participated in the Iranian Thamar Reservoir attack, in which a variety of Israeli targets, including retired generals and employees of defense consulting firms, were targeted using social engineering techniques.[79]

In 2016 Hezbollah successfully hacked the closed-circuit security camera systems in government buildings in Haifa and Tel Aviv, including the IDF's General Staff Headquarters and the Defense Ministry at the Kirya (the Israeli equivalent of the Pentagon), and released the images on social media platforms. Although not a particularly sensitive breach, the attack did enable Hezbollah to monitor those entering the compound and, more importantly, gave it a propaganda coup.[80]

In 2021, in an apparent outgrowth of the Lebanon-based training camps, a Hezbollah-affiliated hacking group, the Cedars of Lebanon, exploited vulnerabilities in Oracle and Atlassian servers to attack approximately 250 telecommunications, web hosting, and infrastructure firms, as well as other targets, in Israel, the United States, UK, Egypt, Jordan, Saudi Arabia, UAE, Palestinian Authority, and more. Once inside the systems, most of the attacks proceeded manually, but in some cases additional tools were installed, enabling the hackers to gain remote control over them. Some of the code was the same as that used by Iranian hacker groups, thereby indicating cooperation between them. The Cedars of Lebanon were first uncovered in 2015 but succeeded in operating under the radar in the following years, partly by employing widely used tools that did not leave a unique footprint.[81]

In 2022, Iran and Hezbollah conducted a cyber espionage attack against the UN force deployed in southern Lebanon (UNIFIL) in order to restore Lebanese

sovereignty in the area and serve as a buffer between Hezbollah and Israel. The attack sought to gain information about UNIFIL's deployment and operations, as part of Hezbollah's and Iran's ongoing activities against Israel.[82]

CNI attacks—information operations have long been a critical part of Hezbollah's multi-decade strategy of asymmetric attrition of Israel's capabilities and societal resilience, to ultimately effect its destruction. Hezbollah has used the cyber realm to augment information campaigns designed to promote international pressure on Israel to prematurely cease military operations, before it had achieved its objectives,[83] and adversely affect its international standing. Indeed, Hezbollah leader Hassan Nasrallah is reported to believe that cyber information campaigns have come to be even more effective for Hezbollah's purposes than military operations.[84] Beyond this, details are sparse.

Palestinian Islamic Jihad (PIJ)—for two full years, between 2012 and 2014, the PIJ hacked the (unencrypted) communications of IDF drones operating over Gaza, enabling it to ascertain in real-time the intelligence they gathered and facilitate its and Hamas's efforts to hide rockets. Concomitantly, live feeds from Israeli road cameras were hacked in order to ascertain where rockets had fallen and to monitor the movement of IDF forces, thereby improving PIJ rocket targeting. The PIJ also attempted, unsuccessfully, to intercept phone conversations on Israeli carriers.[85]

Another attack allowed the PIJ to track the landing and departure times of airplanes at Ben-Gurion Airport[86] in order to better target rocket attacks on the airport during times of conflict and disrupt Israel's civil aviation. PIJ cyber operatives were trained by Iran in Gaza and, in some cases, Iran itself.[87] The good news, according to one source, was that PIJ did not have the necessary know-how to make effective use of this training in ways that could have seriously affected IDF operations or harmed the civilian population.[88]

Anonymous—a hacktivist "collective" that advocates virtual civil disobedience, social agitation, and chaos, along with various spin-offs, has carried out dozens of highly publicized cyber attacks against targets around the world, including the White House, CIA, MasterCard, PBS, Sony, the Vatican, and AIPAC (American Israel Public Affairs Committee). It has also provided technical support to activists during the Arab Spring and the Occupy Wall Street movement, as well as protesters in the United States enraged over the killing of a black man by a police officer.[89] Some members of Anonymous openly identify as pro-Palestinian, Arab, or Moslem.

Ever since 2012, a subset of Anonymous has launched an annual cyber attack against Israel dubbed #OpIsrael, intentionally timed to coincide with Holocaust Remembrance Day. Ostensibly begun in retaliation for Israel's operation in Gaza that year, the stated aim of the recurring annual attack is to "terminate the Israeli cyber space by any means necessary" as part of an "electronic holocaust." Over

the years, Anonymous has targeted websites and servers operated by the IDF, the Prime Minister's Office, ministries of finance, education, health, tourism, and the environment, Knesset, judiciary, Yad Vashem (Israel's national Holocaust memorial), National Insurance Institute (the equivalent of the US Social Security), Ports and Railways Authority, Antiquities Authority, the Jerusalem municipality, and various financial, business, educational, non-profit, and media websites. The 2016 #OpIsrael attacks were launched from computers in the United States, UK, Germany, France, Turkey, Indonesia, and Lebanon.

Anonymous hackers openly take credit for the attacks and boast about them, at times grossly overstating the harm caused. In one case, they falsely claimed that the attack had led to the release of massive quantities of data and the disruption of over 100,000 websites, at a supposed cost to the Israeli economy of some $3 billion. In reality, most of the attacks have been unsophisticated website defacements, DDoS attacks, and viruses and have caused little harm beyond temporary disruptions. Some cyber experts consider Anonymous too amateurish to be capable of breaching well-defended systems in Israel. Given that the date of the annual #OpIsrael attacks is known in advance, allowing Israel to take defensive measures, their primary motivation may actually be the media coverage that their anti-Israel message generates.

Pro-Israel hacktivists have launched counter attacks against Anonymous that have often proven even more successful and gained more attention than the original attacks and Anonymous has consequently begun losing its luster. Nevertheless, Anonymous-style hackers, or hackers it has inspired, as well as other pro-Palestinian groups and individuals around the world, continue to conduct cyber attacks as part of #OpIsrael and, on a smaller scale, on a daily basis.[90]

The Syrian Electronic Army (SEA)—is a shadowy group of hackers that sprang up in 2011 in support of Syria's President Bashar Al-Assad during that country's civil war. SEA began by launching attacks on websites and targets perceived as hostile to Assad's rule, in some cases with significant results, and later also defaced websites belonging to Western media companies, such as the *New York Times* and BBC. Over time, the group's goals changed, and it briefly also targeted Israel. In 2013, following an Israeli airstrike in Damascus, the SEA claimed that it had attacked the remote control system for Haifa's municipal water system.[91] During the conflict in Gaza in 2014 the SEA launched a number of comparatively sophisticated attacks on Israel's civil infrastructure[92] but failed to cause significant damage, and the attackers quickly pivoted to less sophisticated attacks such as DoS and DDoS. Paradoxically, these attacks proved more effective, successfully defacing and blocking access to websites, such as those of the Home Front Command and the IDF Spokesperson's unit, in some cases posting SEA images on them.[93]

We now turn to the primary cyber threat to Israel, Iran.

5

The Iranian Cyber Threat

The Islamic Republic of Iran must become among the world's most powerful in the area of cyber.

Ali Khamenei, Supreme Leader of Iran

Iran is the primary threat to Israel's national security, in the kinetic and cyber realms alike. Iran is also the leading rival of many of the Sunni states and a highly controversial player on the international stage. Chapter 5 presents a comprehensive picture of the Iranian cyber threat generally and specifically to Israel.

Chapter 5 has four sections. It begins with a discussion of Iran's overall cyber strategy and of the institutions and capabilities that it has put in place to implement that strategy. The second section presents the primary cyber attacks attributed to Iran against actors in the Middle East and around the world; the third section presents the Iranian cyber threat to Israel. The final section addresses a critical question: What is the actual impact of the numerous attacks conducted against Israel to date, whether by Iran, or the other actors presented in the previous chapter? There has clearly been a great deal of action, the actual ramifications are less clear.

Iran's Cyber Strategy, Institutions, and Capabilities

Three primary factors appear to account for Iran's decision to rapidly develop its cyber capabilities in the 2010s. The first was the massive wave of protests following the 2009 presidential elections, in which the regime reportedly rigged the outcome in favor of its preferred candidate. The protesters made extensive use of social media to disseminate information inside and outside of Iran and to keep the movement alive for months after the elections were over. Although the regime succeeded in suppressing them, the protests engendered a new awareness

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0006

on its part of the threat to its stability posed by the rapidly spreading use of cyber technology in Iran at the time.[1]

The second primary impetus, ironically, was the dramatic Stuxnet attack against Iran's nuclear program in 2010 (see Chapter 10), the first known case of a cyber attack that caused physical damage. Reportedly a joint US-Israeli cyber sabotage operation, Stuxnet demonstrated Iran's severe vulnerability and caused a consequent determination to prevent the recurrence of such attacks in the future. To this end, Iran rapidly accelerated the development of its then only nascent cyber capabilities and was on the offensive within just two years, with a series of attacks against the United States, Israel, Saudi Arabia, and other states.[2] A third and later factor was fear of the rise of ISIS in neighboring Iraq and the need to reassure Iranian citizens that their country was not about to succumb to the fast-growing threat.[3]

The actual sophistication of Iran's cyber capabilities today is the subject of debate among experts. While there is little doubt that they have progressed considerably, one school of thought holds that Iran has not yet made the investments necessary to develop a sophisticated cyber security ecosystem and suffers from a massive brain drain. Iran's capabilities are, consequently, not believed to reflect the level of professionalism associated with an advanced state actor, and it thus remains a third-tier cyber power, incapable of conducting warfare-level offensive operations. Although Iran has successfully conducted cyber operations around the world, this school holds that important US, European, and Israeli targets are hardened beyond the capability of Iranian attackers, as a result of which they have focused on the "low hanging fruit," such as spear phishing attacks on email and social media accounts. Given the sophistication of Israel's cyber defenses, these experts believe that Iran's ability to inflict major costs on it may even be diminishing.[4]

Other experts are less sanguine and believe that Iran is now at the top of the second-tier cyber powers, with aspirations to join the global frontrunners. The United States believes that Iran has demonstrated a clear ability to learn from others and has become a significant threat. The former head of the INCD, Yigal Unna, maintains that Iran is one of the few states today that does not just conduct attacks for intelligence and influence purposes, but also for destructive purposes and that it has become one the five most active states in the cyber realm.[5]

A senior former Pentagon cyber official argues, in contrast, that Iran has invested heavily in fostering a technologically savvy population, including significant resources that have been devoted to the development of an ICT infrastructure at schools and universities. In the late 2010s fully 18% of Iranian university students studied computer science, while compulsory military service enabled Iran to channel technologically sophisticated graduates to the state security apparatus, including the Ministry of Intelligence and the IRGC.[6] Siboni argues

that Iran has demonstrated a growing capability to carry out complex cyber operations.[7] Loudermilk believes that Iran's cyber capabilities have evolved to the point that it now takes a sophisticated approach, akin to that of the United States, Russia, and China, and can sustain long-term reconnaissance and espionage operations.[8] The increase both in the number and sophistication of Iranian cyber attacks against Israel in the early 2020s, presented below, lends credence to these harsher assessments.

What is not in dispute, is that Iran's investment and activity in the cyber realm have grown considerably. As early as 2016 Iran was reportedly already spending over $1 billion annually on its cyber capabilities, compared, for example, with $2 billion a year by the UK, one of the world's top cyber powers.[9] According to Iranian data, Iran's cyber budget jumped twelvefold under President Hasan Rouhani and in 2020 the Supreme Council for Cyberspace discussed a five-year plan which, if implemented, was designed to increase Iran's digital economy from 6.5% of GDP that year to 10% by 2025.[10]

In 2012 a Supreme Cyber Space Council was established, responsible for planning and implementing an integrated national cyber strategy,[*] as well as a National Cyber Center, designed to coordinate all of Iran's cyber activities, gather and disseminate relevant information and policy directives, and oversee policy implementation. A National Passive Defense Organization was established to defend critical national infrastructure, while the military (*Artesh*) established a Cyber Defense Command to coordinate military cyber operations. Cyber units were rapidly established by virtually all relevant government agencies and within three years the IRGC claimed to have recruited thousands of personnel.[11] A Computer Emergency Response Team Coordination Center (CERTCC) reportedly recovered 600 attacked websites, protected 3,000 government web pages, and countered 53 malware attacks during the first five months of 2018 alone.[12] All of this complemented the long-existing Ministry of Intelligence and Security, which is responsible for signals intelligence, as well as the Ministry of Information and Communications Technology. Iran was thus one of the first states to establish the organs necessary to implement a coherent national strategy in the cyber realm.

The IRGC is the dominant cyber actor in Iran today, with primary responsibility for offensive operations through its Electronic Warfare and Cyber Defense Organization. The IRGC also provides operational direction and support for the cyber operations of Iranian proxies, such as Hezbollah. The Basij, a paramilitary force under the IRGC responsible for domestic order, claims to have

[*] The council's membership includes the president, speaker of the Parliament, head of the Islamic Republic of Iran Broadcasting, commander of the Armed Forces, commander of the IRGC, minister of defense, minister of information and communications technologies, and others.

1,000 cyber battalions around the country. The Basij outsources cyber attacks to some 50 different groups of hacktivists, each of which operates independently, competes for contracts, and has its own modus operandi and targets. Some of the better known are the Iranian Cyber Army, Islamic Cyber Resistance Group, and Ashiyane Digital Security Team. Other examples are a variety of "Kitten" groups: Flying Kitten gathers intelligence on foreign governments and corporations of interest; Magic Kitten targets domestic dissidents; Domestic Kitten targets dissidents in Iran, the United States, UK, and other countries; Charming Kitten uses social networking platforms to reach various targets; and Cutting Kitten produces website penetration tools. Basij cyber activities are coordinated by the Basij Cyber Council; some are conducted through three "institutes," Mabna, Rana, and Nasr. The Cyber Police (Fata) deal with both cybercrime and domestic suppression, although its official remit is to protect "national and religious identity, community values, legal liberty and critical national infrastructure from electronic attack."[13]

As in other areas of asymmetric warfare, Iran seeks to mask its cyber operations in order to maintain plausible deniability. Members of the various hacktivist groups change continually, blurring the lines between them, and malware that is publicly attributed to Iran is often abandoned upon exposure.[14] Moreover, the command structure between the IRGC, Basij, and various groups is fluid, making their activities particularly unpredictable and difficult to assess. This is further obscured by the opaque nature of the Iranian regime and of the murky control it exercises over the security apparatus as a whole. To further cover its tracks, the IRGC reportedly employs trusted intermediaries to outsource contracts to the hacktivist groups, at times employing several contractors for a single operation. At the very least, the hackers appear to enjoy tacit approval from the political and security establishments.[15]

Some believe that cyber has become a top priority for Iran's national security doctrine.[16] Iran has not, however, issued a comprehensive public statement of its cyber strategy, much as it has not in other areas of national security. Our understanding of its cyber strategy thus derives from bits and pieces of information, partial statements, and a combination of our far greater familiarity with Iran's national security thinking generally and observable praxis, both in the cyber and other realms.

To Iran, the long and bitter adversarial relationship with the United States presents the greatest threat to its national security and the only existential threat to the future of the Islamic Republic. Israel is perceived as a severe and particularly active threat, though not an existential one, and other states in the region are also believed to present significant threats to Iran's security. This severe threat perception is further embedded in a deep-seated national sense of weakness stemming from the failed chapters in Iranian and Persian history and the

recognition that Iran's limited conventional capabilities are no match for those of its militarily superior adversaries.

Iran's national security doctrine is rooted in this pervasive sense of vulnerability and a consequent determination to deter enemies and defend against them, but also to wield effective offensive capabilities to promote Iran's interests and influence. Asymmetric warfare has long comprised a critical component of Iran's national security doctrine and the primary means by which it has sought to offset the advantages of its more powerful adversaries. Cyber also fits in particularly well with Iran's strategic culture, which emphasizes ambiguity and deniability, including the use of proxies.[17] Iran has thus sought to develop a variety of offensive cyber capabilities, in CNA, CNE, and CNI.

Much like China, North Korea, and other authoritarian states, Iran has an ambivalent attitude toward the Internet. On the one hand, it views the Internet as a subversive means of propagating Western values and thus a threat to regime survival—the Islamic Republic's foremost objective. On the other hand, it also views the Internet as a means to shape the views of the Iranian people and as an instrument of popular control. To this end, Iran has become a world leader in website filtering and blocking technologies and has gained relatively effective control over the national cyberspace. Iran has also devoted considerable effort to creating a sizable and effective cyber propaganda machine.[18]

Following the Chinese example, Iran established a separate national intranet, called the National Information Network (NIW).[19] The NIW project began in 2009, when Iranian authorities instructed domestic companies to begin moving their network activities to servers and data centers located on Iranian soil, with the objective of ultimately hosting all Iranian websites there. It was later reported that Iran was also developing an independent email service, operating system, search engine, and other tools for use on the network.[20] By 2018, one of whose principal designers is owned by the Revolutionary Guards, the NIW consisted of approximately 500 government-approved national websites that stream content far faster than those based abroad. To encourage use of the NIW, providers offer cheaper packages to customers that access it solely, rather than the Internet.[21] The NIW was officially completed in 2016, but in practice work is ongoing. In 2020 a new cloud infrastructure project and data center for the NIW were inaugurated.[22]

The NIW has enabled the regime to better block what it considers to be pernicious cultural and political influences emanating from the West and Israel, monitor and identify sources of malicious activity, and reduce its vulnerability both to external cyber attack and domestic opposition. Part of the problem is self-inflicted. In 2014 some 2 million Iranians had smart phones. Today, following government encouragement, there is one for nearly every citizen, but since some have more than one phone, that means that about half of the population has

one. In 2014[23] and especially in 2019, at the height of the protests that year, possibly the greatest challenge to the regime since the revolution in 1979, the NIW was used to shut down Internet access throughout the country for a week. In so doing, the regime was able to prevent the opposition from further mobilizing and hide evidence of the extraordinary measures it had taken to suppress it, including the reported killing of hundreds and jailing of thousands more.[24]

The NIW was used once again in 2022, on at least two occasions, to limit Internet access and make it difficult to share footage and organize protests. In one case, demonstrations broke out following the collapse of a building in the already restless Khusestan province, in which dozens died. In the other, when demonstrations spread to tens of cities throughout Iran, following the death of a woman arrested for failing to wear her hijab properly, the Internet was shut down at times and mobile internet connections, as well as Instagram and WhatsApp, two of the most popular social media services in Iran, were disrupted.[25]

For Iran, cyber does not constitute a standalone but an additional capability, designed to complement other capabilities: diplomatic, political, economic, and military. On the military level, Iran views cyber as a means of augmenting and amplifying an array of more traditional asymmetric capabilities, such as terrorism, as well as the buildup of Hezbollah's military capabilities in Lebanon and of Iran's own military presence in Syria. As is true of global powers and other regional actors active in the cyber realm, Iran perceives it as a realm in which it can act with comparatively little risk of retaliation and escalation, certainly kinetic, whether during the protracted periods of low-intensity conflict with Israel or the shorter, but sharp, periods of heightened military tension between Israel and Iran's proxies and allies. Cyber is particularly attractive as a tool of asymmetric warfare because the United States, Europe, and Israel are far more cyber dependent than Iran is and therefore more vulnerable to attack.[26] It is not known if and how cyber fits in with Iran's nuclear strategy.

Iran's cyber operations to date have comprised a mixture of deterrence and disruption to warn off and punish adversaries, espionage for intelligence collection and domestic suppression, and information campaigns directed at foreign and domestic audiences. These operations have been designed to achieve a number of strategic objectives: to ensure regime survival and defend Iran against foreign attack, first and foremost; to promote Iran's ideology, influence, and presence abroad; to counter US efforts to isolate Iran and undermine its influence in the region and make the cost of staying untenable; to make it harder for the United States and its allies to take concerted action against Iran, especially over the nuclear issue;[27] and to promote Iran's objectives vis-a-vis Israel.

An IRGC cyber defense system, reportedly developed with Russian and possibly Chinese assistance, is thought to have become operational in 2015.[28] In 2015 Russia and Iran concluded an initial cyber cooperation agreement, rapidly

followed by a number of more substantive ones. In 2016 they agreed to cooperate on "de-monopolizing . . . unilateral Western domination" of software, possibly reflecting Iranian interest in a Russian alternative to Microsoft's Windows and Office software. In 2017 an MOU on ICT cooperation included "Internet governance, network security . . . and international Internet connection." In 2018, at Iran's behest, a bilateral committee was established on media cooperation, including exchanges of journalists, mutual favorable media coverage, coproduction of content, countering Western media narratives, and cooperation targeting foreign audiences, all designed to combat what Iran has called Western media terrorism.[29]

In 2019–2020 bilateral working groups discussed a Russian offer to provide Iran with the equivalent of Moscow's "smart city" project, which allows authorities to track citizens through facial recognition and other technologies, 5G networks, artificial intelligence, and investment in Iranian cyber firms, including possible multilateral investments together with Turkey and Azerbaijan. In 2020 agreement was reached to counter "increasing information pressure from the West . . . designed to discredit Russia and Iran."[30]

An even more robust Information Security Cooperation Pact, signed in 2021, reportedly covered cyber security and technology transfers, including means of detecting attacks; suppression of internal dissent; and coordination in multilateral forums, especially the UN, to promote international cyber norms and law friendly to authoritarian regimes and to counter the Western model of an open and free Internet. The agreement may also provide for a strengthening of Iran's offensive cyber capabilities, although some sources believe that mutual suspicion and diverging goals are likely to have restricted its focus primarily to defensive measures and intelligence sharing. A further danger is that technologies and methodologies acquired from Russia could be passed on to Hezbollah and other Iranian affiliated militias in the Middle East.[31]

All this notwithstanding, the Russian-Iranian cyber relationship has not always been collaborative. Between 2017 and 2019 Russian hackers apparently piggybacked on an Iranian cyber espionage operation in order to attack military, governmental, scientific, and industrial targets in tens of countries, while making it appear that the attacks originated from Iran.[32]

Chinese firms have also invested heavily in Iran's cyber infrastructure. In 2021 China and Iran concluded a major 25-year strategic cooperation agreement that provides, inter alia, for Chinese help in building Iran's 5G telecommunications infrastructure, access to China's new Global Positioning System, Beidou, and help in asserting greater Iranian control over its cyberspace, possibly further strengthening the NIW. China may have agreed, both in the 25-year agreement and previously existing ones, to provide Iran with new cyber capabilities, including those necessary for intelligence gathering purposes, and may share in some of the information collected.[33]

Iranian Cyber Attacks around the World

CNA attacks—in 2012–2013, in response to the Stuxnet virus, Iranian hackers launched the Abadil attack against 46 major US financial institutions, including J.P. Morgan, Chase, Wells Fargo, and American Express, freezing customers out of their accounts. The immediate cost was mostly reputational—diminished customer faith in the ability of these institutions and of the US banking system in general to provide them with secure financial services. In the longer term, the cost was immense, as the US financial industry was forced to spend billions of dollars on highly sophisticated cyber defenses.[34]

The Iranians also succeeded in gaining control over the floodgates of a dam in New York, generating deep concern over their ability to cause potentially severe damage to critical infrastructure. The attack was subsequently found to have actually been of limited consequence, but it had a strong impact on US governmental thinking. By 2021 US intelligence assessed that Iran did have the ability to attack critical US infrastructure.[35]

In 2012 Iran was behind one of the most destructive cyber attacks ever, against Saudi national oil company Aramco. Like Stuxnet, the Shamoon attack caused physical harm, not just a disruption of service, nearly obliterating Aramco's corporate IT structure. Roughly 30,000 computers and 10,000 servers were damaged, forcing the company to shut down its internal network for a week and bringing it to the verge of collapse. Aramco was unable to process transactions, company officials had to use typewriters and faxes to keep billions of dollars' worth of oil trades from falling through, and for a few days the company was even forced to give oil away for free. A similar attack was conducted shortly thereafter against Qatar's natural gas authority. The Shamoon malware resurfaced in 2016, erasing data from thousands of computers in Saudi Arabia's Civil Aviation agency and other organizations; in 2017 it was used against 15 Saudi government agencies and organizations; and appeared yet again in 2018, this time targeting oil, energy and telecommunications firms, and government organizations.[36]

In 2013–2014 an Iranian cyber attack took control of 16,000 computer systems in the United States, UK, and other parts of the world. Another attack breached the networks of airlines, energy and defense firms, and the Intranet of the US Navy and Marine Corps.[37]

The 2015 nuclear deal (formally known as the Joint Comprehensive Plan of Action—JCPOA) was a particular focus of Iranian cyber activity. Prior to the JCPOA, which led to an easing of tensions with the United States and the West, Iran had reportedly been poised to attack US and European electric grids, water

plants, transportation systems, financial institutions, and more.[38] Another attack disrupted and destroyed data on the networks of a Las Vegas casino, owned by an outspoken supporter of Israel and critic of the nuclear deal. The US withdrawal from the JCPOA in 2018 and the subsequent policy of "maximum pressure," spurred heightened cyber attacks, including destructive attacks that erased computer data from over 200 infrastructure, aviation, manufacturing, and engineering firms in the United States, UK, Germany, Saudi Arabia, India, and other countries.[39]

In 2021 a secretive Iranian cyber unit, Intelligence Group 13, planned an attack against critical infrastructure targets in a number of Western countries, although it is unclear whether it intended to actually attack at the time or was collecting intelligence for future use. Other attacks under consideration by the unit were designed to affect the automatic gauges of gas station tanks, which could have caused explosions, disrupt cargo ships' ballast water systems, potentially causing them irreparable harm, and disrupt maritime communications.[40]

In 2021 Iranian government-backed hackers sought to damage the computer systems of the Boston Children's Hospital, one of the largest pediatric hospitals in the US. The motive of the attack was unclear, but could have severely degraded or even shut down hospital operations, including ongoing care to patients and emergency surgery. The attack was thwarted before it had the potential to evolve into a ransomware attack.[41]

In 2022, in the first known case of a country severing diplomatic relations over a cyber attack, Albania did so in response to an Iranian ransomware attack designed to disrupt and damage numerous governmental websites and digital services. The attack may have been a response to a conference scheduled to take place in Albania by a leading Iranian opposition group, Mujahideen-e-Khalq.[42]

CNE attacks—at the height of the negotiations leading up to the JCPOA, Iranian hackers breached the personal email accounts of the US negotiating team and other US officials, Congressional critics of Iran, and members of the media. Following the US withdrawal from the agreement, Iranian attacks included cyber espionage operations against senior Treasury, State, and DoD officials involved in the imposition of sanctions, as well as the theft of corporate secrets from the 200 infrastructure, aviation, manufacturing, and engineering firms mentioned above.[43] In 2021 academic experts from a prestigious UK university, in reality Iranian hackers, invited US and British experts to a conference on Mideast security. Once the targets clicked on a "registration link," the attackers gained access to their computers and were able to search for information about their countries' foreign policy, especially on the nuclear issue.[44]

In 2016 Iranian hackers began a wave of attacks against Internet service providers, telecommunications companies, and other targets in Persian Gulf states, which later expanded to government agencies in 12 European

countries and the United States. In the UK, the login details of 1,000 Members of Parliament and their staffs, over 1,000 Foreign Office officials, and 7,000 police were compromised in 2017. The same hackers targeted the Australian Parliament in 2019, as part of a multi-year cyber espionage campaign, as well as governmental, diplomatic, and military websites in Canada and New Zealand.[45]

An IRGC cyber attack against US aerospace and satellite technology firms, which began in 2014 and continued until it was discovered in 2019, used social engineering techniques to steal sensitive information from a target list of more than 1,800 accounts.[46] A major Iranian cyber espionage campaign, between 2014 and 2020, reportedly capable of outsmarting the encrypted messaging systems on applications such as Telegram and WhatsApp, spied on Iranian dissidents, as well as religious and ethnic minorities, at home and abroad, including the United States, Canada, and the EU.[†47]

In 2018–2019 Iranian-affiliated hackers, posing as recruiters from LinkedIn, Cambridge University, and other institutions, sent emails offering attractive, apparent job opportunities as a means of delivering malware to employees at Middle Eastern governments and private firms, including public utilities and oil and gas firms. In 2021 the same group exploited Facebook accounts for similar purposes, posing as employees of hospitality, medical, airline, and other firms. In some cases, they even conversed with their US, UK, and European targets for months at a time and across various social media platforms.[48] That same year, Iran's "recruitment" efforts took a particularly sinister turn, as hackers attempted to gain sensitive expertise and technology needed to build weapons of mass destruction. In what the German government described as a "major cyber attack campaign," German, Swedish, and Dutch employees were sent "job offers" with malware attachments.[49]

In 2019 Microsoft blocked 99 websites used by Iranian hackers to conduct multi-year cyber attacks against government agencies, businesses, and individuals in Washington, DC. That year, Iranian hackers also set up a fake website ostensibly designed to serve the needs of US military veterans transitioning back to civilian life, but which actually downloaded malware that the Iranians apparently hoped would provide access to Pentagon information systems. In mid-2019 US Cyber Command and the Department of Homeland Security grew so concerned about growing Iranian cyber activity against US governmental and commercial targets that they issued a special public warning.[50]

[†] Particularly prominent victims included the Mujahadeen Khalq (MeK), an Iranian opposition organization; the Azerbaijan National Resistance organization, which promotes the rights of Iran's large Azeri minority; residents of Iran's restive Sistan and Balochistan provinces; Voice of America journalists; and a human rights organization.

In 2020 a multi-year intelligence collection operation was discovered that had been used to target Iranian citizens, dissidents, and journalists, as well as governmental networks in the Middle East, foreign academics, and foreign travel and communications firms. At least 15 US firms and individuals were targeted, along with entities from more than 30 different countries in Asia, Africa, Europe, and North America. In a further attack, Iranian affiliated hackers stole "highly protected and extremely sensitive" confidential communications from defense contractors, foreign policy and other NGOs, universities, and the governments of Afghanistan and Saudi Arabia. In 2020 Iranian hackers breached the email accounts of several high-profile attendees at the Munich Security Conference, probably the most prestigious annual gathering of national security luminaries from around the world, as well as the G20 summit held in Saudi Arabia.[51] In both cases, the objective was presumably to gain insights regarding the attendees' views of issues of interest to Iran.

In 2021 two further cyber surveillance campaigns were discovered, targeting over 1,200 dissidents, opposition forces, and Kurds in Iran, the United States, UK, and other countries. The first reportedly used an Iranian blog site, Telegram channels, and text messages to lure targets into downloading malicious software onto their mobile phones. Some 600 victims in seven countries were successfully infected. A second attack, which started in 2007 by targeting domestic targets, was expanded to spy on dissidents and other targets in 12 foreign countries, including Sweden, Denmark, the Netherlands, United States, Iraq, and India. Fake emails with interesting attachments were used to lure targets into downloading the malicious spyware. An innovation introduced in 2020 included the use of a second stage payload for purposes of persistence, surveillance, and data exfiltration.[52]

APT42, apparently a subset of Charming Kittens, conducted two attacks on academic targets in the UK in 2021. In one, dubbed "Operation SpoofedScholars," the hackers impersonated scholars from the University of London's School of Oriental and African studies (SOAS) in order to gleen information from Middle East affairs experts in the US and UK. In the other, APT42 impersonated a legitimate British news organization to target professors in Belgium and the UAE who had ties to the local government or relatives in Iran. A customized PDF document that invited the professors to participate in an online interview, was used for purposes of credential harvesting.[53]

CNI attacks—Iran is engaged in extensive cyber information campaigns against the United States, Saudi Arabia, and other countries. To this end it has operated 70–100 news websites, a YouTube channel, and a mobile phone app store in tens of countries and in a similar number of languages.[54] In these campaigns, Iran portrays itself as a responsible and benevolent member of the international community that sides with the oppressed against an aggressive

camp led by the United States, together with Israel, the Gulf monarchies, and European allies. In contrast with the hypocrisy and double standards of Western foreign policy and US reliance on brutal military and economic force, Iran's power is said to stem from the righteousness of its faith, values, and positions.[55]

Fake Iranian websites create, disseminate, and amplify content geared toward the US and other publics. In 2011 Iran began a social media disinformation operation to promote pro-Iranian positions, support for those US policies deemed favorable to Iran's interests such as the nuclear negotiations, and a variety of anti-Saudi, anti-Israeli, and pro-Palestinian themes. In 2018, capitalizing on the murder of Saudi journalist Jamal Khashoggi, Iran created bots and fake news sites and Twitter profiles to further increase public pressure on Saudi Arabia and undermine the Saudi-US relationship. A sprawling social media campaign during 2019–2020 criticized President Trump's decision to withdraw from the nuclear deal and his policies toward Israel, Yemen, and Syria. By 2020 the campaign had reached millions of people on Facebook, Twitter, Instagram, and YouTube.[‡56]

In 2020 the United States seized 92 domains used by the IRGC to spread disinformation across the world, four posed as genuine news outlets designed to influence US domestic and foreign policy.[57] The American Herald Tribune, actually an Iranian website, paid Americans to publish English-language material that aligned with Iran's views. The articles were then used for purposes of "circular amplification," with Iranian state media publishing or referencing them as examples of Americans supposedly supportive of Iran's positions. Other information operations focused on key ethnic and sectarian groups in Iraq, Lebanon, the Persian Gulf, Syria, and Afghanistan.[58]

Iranian information operations also seek to sow dissension within and between adversaries. To this end, Iran has used social media in the attempt to further exacerbate existing racial, socioeconomic, and political tensions in the United States, often creating a narrative that links them to Iran's own struggles against it. Following the brutal killing in 2020 of a black American by a police officer, who had pressed his knee against his neck until he died of asphyxiation, President Rouhani stated that the United States had its knee on Iran's neck as well. Iranian leaders, including the Supreme Leader, Khamenai, have repeatedly tweeted their identification with the Black Lives Matter movement, presenting both the Iranian and American peoples as victims of an oppressive US government. Iran has also used the Black Lives Matters movement to emphasize

[‡] Twitter identified and removed 7,896 accounts originating in Iran and responsible for approximately 8.5 million messages. Facebook identified nearly 800 fake pages directly related to Iran, or backed by it, with 5.4 million users. It also identified 55 groups joined by 140,000 people, designed to influence public opinion in 28 countries, including Egypt, Libya, Saudi Arabia, France, Germany, the United States, a number of countries in central and South America, and Israel.

alleged American hypocrisy; whereas the United States criticizes Iran for human rights violations, US citizens have to fight for the rights of ethnic and religious minorities, women, and the LGBTQ population. Europe, too, has been held to be hypocritical for remaining silent over US human rights violations, while vocally criticizing Iran's.

Iran has attempted to interfere in US elections ever since 2012. In 2016, Hillary Clinton was seen as tough on Iran and so Iranian linked accounts sought to boost the campaign of her Democratic primary rival, Bernie Sanders. In 2018 Iran interfered in the midterm elections, impersonating US voters and political candidates. Twitter alone shutdown over 7,000 fake accounts. In 2020 Iran intervened more directly in the attempt to sway the outcome in favor of Joe Biden and to prevent the re-election of its nemesis, Donald Trump, who had withdrawn from the nuclear deal, imposed severe sanctions on Iran, and it feared, might pursue regime change in a second term.

Building on techniques already employed by Russia, IRGC hackers sent out tens of thousands of intimidating emails to voters in three swing states, ostensibly from far-right pro-Trump groups. Democratic voters, whose information the hackers had gained through a misconfiguration in a registration database, were warned: "You are currently registered as a Democrat and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on election day or we will come after you." The IRGC hackers also sent out emails containing a deceptive video designed to undermine voter confidence in the electoral process, playing on fears that Trump himself had instigated by claiming that mail-in ballots were subject to fraud. Both the Trump and Biden campaigns were hacked by Iran as well.

Following the elections, Iranian efforts to promote discord in the United States continued. An Iranian affiliated website, Enemies of the People, issued death threats against elections officials and governors who had refuted the claims of voter fraud, as well as the director of the FBI and the senior cyber official in the Department of Homeland Security.[59]

Iran has reportedly also sought to spread domestic dissension in the UK, promote anti-Saudi and anti-Israeli sentiment there and undermine support for the global war on terrorism. An Iranian affiliated "Free Scotland" Facebook page, which promotes Scottish independence, has more than 20,000 followers. A variety of fake left-wing sites, including one entitled Britishleft.com, promote the anti-Saudi and anti-Israel themes. Another site, allegedly based in Birmingham, promotes material repurposed from an Iranian state-owned media network. The cyber information campaign is part of a broader effort to affect political thinking in the UK, including by investment in a variety of British religious and cultural institutions.[60]

Even so, Iranian disinformation efforts are still not nearly as sophisticated as Russia's. The Iranians, according to one informed source, do not sound authentically American, do not spend the years necessary to develop audiences effectively before beginning to spread disinformation, and do not hide their tracks well.[61]

The Iranian Cyber Threat to Israel

Before turning to the Iranian cyber threat to Israel, a brief background to place it in the broader strategic context of the overall threat that Iran poses to Israel's national security is necessary. For decades, Supreme Leader Ali Khamenai and other senior Iranian officials have repeatedly called for Israel's destruction, referring to it, inter alia, as a "cancerous tumor" that must be removed.[62] In 2014 Khamenai even publicly enunciated a nine-point plan designed to achieve this desired outcome.[63] For Israel, this is far from idle talk; to the contrary, Iran has devoted great efforts and resources to this end ever since the Islamic Republic was first established. Indeed, Iran's carefully calculated approach toward the conflict with Israel, combined with its comparatively advanced society, size, and resources, make it the most sophisticated and dangerous adversary that Israel has ever faced. No responsible Israeli official can afford to underestimate the threat.

Iran's nuclear aspirations are the greatest threat to Israel's national security today and the only potentially existential threat it is likely to face, at least for the foreseeable future. The likelihood of Iran ever actually using nuclear weapons against Israel is probably very low, but the consequences are, of course, potentially catastrophic, and Israel must treat the threat with the greatest gravity. The more plausible threat, however, stems from the greatly enhanced stature and power that a nuclear capability would afford Iran, and which would enable it, together with its proxies, to wage an even more aggressive—but sub-nuclear—confrontation with Israel. Moreover, the mere presence of nuclear weapons, even if just in the background, would risk escalation to the nuclear level in every future regional conflict and for Israel, turn otherwise limited into potentially existential confrontations.

Further exacerbating the situation, if Iran does ultimately succeed in acquiring nuclear weapons, additional actors in the region, first and foremost Turkey, Saudi Arabia, and Egypt, may also seek to do so. A Middle East with multiple nuclear actors is simply a nightmare scenario, with no known remedies. Unlike other nuclear rivals such as the United States and Russia or India and Pakistan, Iran explicitly seeks the destruction of its rival, Israel. Whereas, those powers went to great lengths to prevent or mitigate nuclear crises, nuclear actors in the Middle East are likely to have either no channels of crisis communication whatsoever

or highly limited ones. Furthermore, Iran and Saudi Arabia are theocracies, and even if they probably are "rational actors," the rationality of theocracies may somehow be different, if only in some small but critical measure. The prospects of nuclear weapons actually being used in a Middle East with multiple nuclear actors are truly frightening.

Iran's conventional military capabilities are limited and unlikely to pose a major threat to Israel for some time. Iran does have a significant and rapidly growing arsenal of ballistic and cruise missiles capable of striking Israel, as well as drones, but the primary threat it poses is indirect, through its powerful Lebanese proxy, Hezbollah. Hezbollah and Israel have engaged in a number of confrontations over the decades, none of which have ended satisfactorily from Israel's perspective.

Iran is believed to have armed Hezbollah with a staggering arsenal of up to 150,000 rockets. In a major confrontation in the future, it is estimated that Hezbollah may fire as many as 2,000 rockets at Israel daily, for a period of weeks, which would cause severe damage to its civilian home front.[64] Furthermore, Iran has begun supplying Hezbollah with precise rockets, a possible game changer from Israel's perspective. Precise rockets would provide Hezbollah with the ability to disrupt both defensive and offensive IDF operations, for example, by targeting anti-rocket systems, mobilization centers, and air bases; Israel's command and control processes, by targeting the premier's office, IDF headquarters, and military communications nodes; and its economy and society, by targeting critical national infrastructure. Israel's offensive capabilities and rocket defenses will mitigate the threat but cannot fully neutralize an arsenal of such mammoth proportions. No other Arab adversary has ever had the capacity to cause such disruption to Israel's civil and military rears.[65]

Iran is further engaged in a sustained effort to establish a permanent military presence in Syria, along with Hezbollah and other allied militias. Israel has been successful so far in slowing this effort but appears to be fighting an uphill battle. Syria's future remains unclear, but it is likely to remain under significant Iranian influence and to constitute an at least partial forward operating base against Israel for both Iran and Hezbollah. The ramifications for Israel are severe and could lead to a direct military confrontation with Iran, above and beyond the indirect confrontation already underway in the Lebanese and Syrian arenas. It also risks a rift in Israel's relations with Russia, the other primary player in Syria, and which has deployed there its most advanced anti-aircraft systems and established air and naval bases. Iran has also deployed missiles in Iraq and Yemen capable of reaching Israel.

In contrast with Israel's Arab adversaries in the past, Iran and Hezbollah do not seek its defeat in the near term, which they know to be beyond their capabilities, and have instead adopted a long-term strategy of "attrition until destruction."

In so doing, they make use of a variety of weapons and tactics designed to partially neutralize Israel's technological superiority, prevent it from achieving victory, and demoralize its population. To this end, Hezbollah intentionally places rockets among its civilian population, making it very difficult to locate and destroy them and forcing Israel to cause civilian casualties when it seeks to do so, and creating international pressure on Israel to end the fighting before it has achieved its military objectives. At the same time, Hezbollah's own offensive efforts are focused overwhelmingly on Israel's civilian population through massive and protracted rocket attacks.[66]

Iranian Cyber Attacks against Israel

Iran has become the primary threat to Israel in the cyber realm, as in all others. The following section provides a detailed account of the cyber attacks that Iran has conducted against Israel. In some cases, these were parts of broader campaigns launched against multiple states. Some were also cross-cutting, that is, they combined elements of CNA, CNE, and CNI attacks, as well as cyber crime. The attacks have been classified in the following account according to their primary intent.

CNA attacks—in 2012, in one of the first Iranian-affiliated cyber attacks against Israel, directed in this case at the Israel Police, external connections to servers had to be shut down and each network isolated until the servers could be scrubbed clean. The process took a large team, working 24 hours a day, a full week to complete,[67] supporting the contention that the impact of cyber attacks is not always transient even once they are discovered.

During the conflict with Hamas in 2014, a large-scale Iranian attack was launched against Israel's civilian communications system,[68] one of the earliest reports of an attack on critical national infrastructure. Iranian hackers also attempted to flood a core piece of Israel's Internet infrastructure, the DNS, which acts as the web's directory or "phone book" and is critical to its operation.[69] The Israel Internet Association, which is responsible for the national DNS, was subsequently defined as critical national infrastructure.

In 2015 or 2016, the precise date is unclear, Iranian hackers reportedly believed that they had successfully conducted a massive attack on Israel's power grid and possibly even a nuclear facility. The computer networks attacked were actually decoys, also known as honey-pots,[70] designed to deflect attacks and expose attackers' intentions and capabilities. Nevertheless, it is the very fact that the attackers may have been willing to carry out such potentially escalatory attacks that is of concern. Moreover, as seen below, this was not the only nuclear-related Iranian cyber attack against Israel.

In 2018 Iran attempted to hack the Home Front Command's systems for warning the public about rocket attacks. Had they succeeded, they would have been able to declare false alerts or even worse, prevent the national alert system from being operated to warn the civilian public.[71]

There was a dramatic upturn in Iranian, or Iranian-affiliated, cyber attacks against Israel in 2019–2021, part of a series of blows and counter blows between Iran and Israel that was then in full blast. The Iranian attacks came in waves: in July 2020, 19,000 cyber attacks were launched against Israeli firms with 33,600 launched in November.[72]

In another wave, which began in 2019 and continued through the spring of 2020, a series of attacks was launched against Israel's water supply and waste management system, apparently by the IRGC. Israel succeeded in thwarting the Iranian campaign until April 2020, when an attack launched via US-based servers disrupted, or gained control over, the computerized control systems of six water, sewage, and sewage treatment stations. Israel's cyber defenses rapidly detected the attack, and no actual harm was caused, but an attack on such a sensitive infrastructure system caused considerable shock. Had Israel's defenses proven less effective, the attackers would have been able to increase the quantity of chlorine and other chemicals injected into the water supply to life-threatening levels and possibly cause a national shortage in drinking water. Other water facilities around the country were immediately ordered to change the passwords of their operational systems. Following the attack, the INCD established a special sectoral Security Operations Center (SOC) for the water system, although many of the regional water firms had yet to join it a year later.[73]

The importance Israel attached to the attack was further demonstrated by a special meeting convened by the security cabinet and by an unusual statement by the head of the INCD, Yigal Unna, who defined it as a "turning point in the history of modern cyber warfare." Unna further stressed that this was the first time that Israel's cyber adversaries had ever attempted to cause lethal physical damage, rather than confining impacts to the cyber realm. He concluded the statement with a chilling message:

> Cyber winter is coming and coming faster than I expected . . . It seems like there are some new rules of engagement, rules of war in cyber warfare . . . If in the past we believed that there were (red) lines that should not be crossed, in this case all of the lines were crossed and they may be again in the future.[74]

Just weeks later two more limited attacks once again targeted Israel's water system, one against agricultural water pumps in the upper Galilee, the other against infrastructure in the center of the country. In the attempt to frustrate

Israel's defenses, the attacks were conducted by means of Iranian code sent via American and European servers. Neither caused damage,[75] but their very occurrence demonstrated that the counter strikes that Israel had reportedly launched in response to the earlier attacks had failed to achieve the intended deterrence.

Another wave of attacks in 2020, conducted by the Hackers of Saviors, an Iranian-affiliated hacktivist group that ostensibly seeks to promote the Palestinian cause, was timed to coincide with Iran's al-Quds (Jerusalem) Day. Despite a warning issued by the INCD a week earlier that an attack of this type and timing was expected, the Iranian hackers successfully exploited a cyber security weakness in the servers of UPress, a leading Israeli hosting site, and defaced thousands of websites, replacing them with vicious messages, including calls for Israel's destruction. They also sought to induce users into downloading malware that would have completely erased their data. The targeted websites included municipalities, private firms, including a pharmaceutical company and food chains, not for profit organizations, and a regional water authority.[76] Arguably most egregiously, the business website belonging to the spouse of one of the authors of this book was also disrupted.

Still another attack at the time focused on the IDF's civilian supply chain, including gas and food vendors. The activities and modes of operation of vendors such as these can provide important insights into IDF operations.[77]

MuddyWater, another Iranian-affiliated hacking group, launched what appeared to be a precursor to ransomware deployment but may have actually been preparation for a large-scale destructive attack. Agrius, still another Iranian-affiliated hacking group, launched what was initially a cyber espionage campaign but evolved into destructive wiper attacks. Agrius also launched a "password spraying" CNE campaign against the Office 360 accounts of US and Israeli defense firms involved in the manufacture of satellites, drones, radar, and other equipment; twenty firms were successfully compromised.[78]

In 2021 Siamese Kittens launched a supply chain attack against Israeli IT and communications firms. The attackers posed as fellow IT and communications firms, including their human resources personnel, as a means of luring the Israeli IT experts into compromising their computers and gaining access to them. The attack may have been in preparation for deployment of wiper malware or ransomware.[79]

The year 2021 saw ransomware attacks against nine Israeli hospitals, possibly by the same Iranian hackers who had conducted the attack that year against the Boston Children's Hospital. With the exception of Hillel Yaffe, where some 36 million shekels in damage was caused, (approximately $10 million), the other hospitals successfully repelled the attacks. The attack against Hillel Yaffe paralyzed the majority of its computer systems, forcing the hospital to use alternate systems, record patient information by hand and redirect new patients, who

were not in need of urgent care, to other hospitals. The point of entry for the attack may have been a weak or outdated VPN software used by the hospital. Initially attributed to Chinese hackers, it took the hospital a month to recover. Damage to the hospital's computer systems was so extensive that the IDF Cyber Defense Brigade was forced to provide assistance.[80]

In 2022 the Hackers of Saviors disrupted the logistics operations of the Gold Bond firm at the port of Ashdod. The attack may have been a retaliation for a similar but far more severe attack, allegedly conducted by Israel against an Iranian port the year before (see Chapter 10) following the attack on the national water system mentioned earlier.[81]

In 2022 the INCD declared a state of emergency following a cyber attack of unprecedented size and scope that succeeded in temporarily disrupting the websites of a number of government ministries, all part of the government Internet portal gov.il. The websites attacked included the Premier's Office, Foreign Ministry, and Ministries of the Interior, Health, Justice, and Social Welfare. Critical infrastructure sites, such as the electric grid and water system, may have also been attacked, although this had not been confirmed at the time of this writing. A Telegram account affiliated with Iran's Revolutionary Guards took credit for the attack.

In practice, this was an unsophisticated DDoS attack; all of the websites were able to restore service after a brief period and no damage was caused. Significantly, the websites of the Ministry of Defense and the defense establishment are not part of the gov.il portal and were not attacked. The attack appeared to be part of the heightened exchange of both cyber and kinetic attacks between Israel and Iran in the spring of 2022, including Iranian claims that Israel had sought to sabotage the Fordow nuclear facility, destroyed hundreds of Iranian UAVs in another attack, and killed two Revolutionary Guards, apparently involved in Hezbollah's precision rocket project, in still another one.[82]

Iranian-affiliated hackers launched a DoS attack in 2022 that temporarily disrupted the website of the company building Tel Aviv's new light rail line. Still another group has targeted Israeli shipping, including potentially sensitive components. Unidentified hackers, Iranian or otherwise, exposed an open and undefended control system of the Or Akiva municipality's sewage system. Had they so wished, the hackers could have taken control of the system, opening or closing pumps and valves at will.[83]

CNE attacks—Iranian cyber espionage attacks have focused on defense officials, defense industries and nuclear scientists. Iran has also repeatedly sought to gain insights into Israeli strategic thinking through CNE attacks against Israeli academics who have links to the defense establishment. To this end, Iranian hackers have posed as the academics' colleagues and personal acquaintances, seeking to gain their unvarnished assessments beyond that which appears in

published papers. In order to make the attacks appear credible, the attackers studied ongoing email exchanges and even participated in some.[84]

In some attacks, the targets were mostly located in other countries and only secondarily in Israel. In 2011 Iran launched Newscaster, reportedly the most elaborate social media spying campaign it had conducted up to that time. By creating a series of virtual identities on Twitter, Facebook, and other social media sites and setting up a phony news site, the hackers were able to pose as journalists with close ties to government officials and gain potentially sensitive information regarding the US-Israeli relationship, the nuclear negotiations then underway, weapons development programs, and defense issues generally. Altogether, more than 2,000 computers were compromised, mostly in the United States, including hundreds of senior defense, diplomatic, and other officials, both current and former. Officials from over 10 US and Israeli defense contractors were also targeted. The attack was not discovered until 2014.[85]

Copy Kittens has targeted Israel ever since 2013, as well as the United States, Saudi Arabia, Turkey, Jordan, and Germany, focusing primarily on governmental agencies, defense and IT firms, academic institutions, and municipal authorities. The first step of each such attack was an infected email attachment, usually carefully chosen to match the target's interests.[86]

Between 2013 and 2017 Iranian hackers launched a campaign of cyber intrusions into the computer systems of 320 universities, mostly in the United States but also in Israel and other countries. Altogether, the hackers targeted the accounts of more than 100,000 academics, successfully compromising approximately 8,000 and stealing a vast quantity of data and intellectual property.[87] In 2018 a further attack on 76 universities in the United States, Israel, and elsewhere was uncovered. Once again, the attackers sought to steal unpublished research and obtain intellectual property.[88]

In the Thamar Reservoir attack, which began in 2014 or possibly as early as 2011,[89] Iranian hackers reportedly used spear phishing and social engineering techniques, such as phony websites and fake messages on social media, to persuade targets to install malware. In this case, the hackers sought access to the social media and email accounts of retired Israeli generals, defense consulting firms, and academics, sending malware attachments disguised in Word and Excel files. The malware contained "keyloggers," computer code that enabled the hackers to record every keystroke made by the users, take screenshots, and copy files, all without their knowledge.[90]

Starting in 2014, Rocket Kittens repeatedly targeted Israeli academic institutions, defense contractors, and more, as well as other targets across the Middle East. In a number of cases, Rocket Kittens impersonated Israeli engineers, including a particularly well-known one, to provide legitimacy for the attacks and increase the probability that targets would download the infected

malware. A variety of techniques were employed, such as Facebook and SMS messages and spear phishing emails. The attacks were not very sophisticated and included easily identifiable errors, but were notable for their persistence. In effect, the attackers sought to simply overwhelm the targets with attacks until someone eventually erred and downloaded the malware.[91]

In 2015 an unknown attacker, presumed to be affiliated with Iran or possibly Hezbollah, sent emails to officials at the Ministry of Defense containing "keyloggers." The infected messages were opened by a few employees allowing the attacker to successfully accessed the ministry's unclassified network, but not its classified one, and the ministry's cyber security unit was able to swiftly neutralize the attack.[92]

In 2017 Copy Kittens launched Operation Wilted Tulip, masquerading as the Prime Minister's Office and Israeli news sites, to target Israeli embassies abroad and foreign embassies in Israel. The group was careful to use infrastructure located largely outside of Iran, in the United States, Russia, and the Netherlands.[93]

In 2017 the Oil Rig hacking group disguised itself as a well-known Israeli software firm and sent malicious emails to 120 Israeli government agencies, academic institutions, computer firms, and individuals using a fake security certificate. The phishing attack exploited vulnerabilities in Microsoft Word to gain access to the address lists of the targeted computer networks, which were then used to further spread the attack.[94] Oil Rig also conducted attacks against at least five Israeli IT vendors, several financial institutions, and the Israel Post Office. In one case, it set up fake websites purporting to be a registration page for a conference at the University of Oxford and a job applications site. In another, the attackers cloned the website of IsraAir, an Israeli airline, and sent targets a malicious Excel file.[95]

In 2018 Iranian hackers reportedly targeted Israeli nuclear scientists in an effort to gain access to sensitive materials. The hackers sent emails to the scientists, as part of a phishing scam, with links leading to a phony British News Agency.[96] According to another report, 11 different IRGC hacking groups were engaged in attacks against Israeli nuclear researchers at the time, on an almost daily basis.[97]

In 2020 Iranian hackers posed as General Amos Yadlin, a former head of Military Intelligence and at the time the head of INSS, Israel's foremost strategic affairs think tank. The attack took the form of a request, from what appeared to be Yadlin's personal WhatsApp number, that a scholar at another institute comment on an INSS study that had yet to be published and which the attackers had clearly obtained surreptitiously.[98]

In 2019 a dangerous change occurred in Iranian CNE attacks. An Iranian-led group, operating out of Syria, used Facebook and messaging apps in an attempt to recruit agents in Israel, apparently in preparation for terrorist attacks. Most

of the Israeli targets grew suspicious and severed contact. Iran was reportedly also behind attempts at the time by Hezbollah and Hamas to use the Internet to recruit Israeli Arabs and Palestinians for purposes of terrorism and intelligence gathering in Israel.[99]

In 2021 Iranian intelligence used Instagram accounts, impersonating attractive women, to try and lure Israeli businessmen into meetings abroad, for business and/or romantic purposes, which were really traps to harm or kidnap them.[100] That same year, an Iranian-affiliated operation exfiltrated large amounts of data about Israel and other targets in the Middle East, United States, Europe, and Russia from global aerospace and telecommunications companies. The highly targeted campaign, which had apparently begun at least three years earlier, succeeded in remaining under the radar by using a previously undiscovered Remote Access Trojan that evades antivirus tools and other security measures.[101]

An Iranian intelligence officer, posing as an "Iranian Jew," used Facebook and WhatsApp to recruit five underprivileged Israeli women of Persian descent to complete tasks for Iran in exchange for money. Among other assignments, two of the women were instructed to encourage their sons to serve in the Intelligence Corps, one was told to collect intelligence on senior defense officials, and still another how to create a compromising sexual situation for a Member of Knesset she was in touch with. They were also instructed to photograph and gather information on a list of targets that might be helpful in carrying out future terrorist attacks. Some of the women involved in the operation, which was disclosed publicly in 2021, had been in touch with their Iranian handlers for years.[102]

A similar attack took place in 2022. The attackers, posing as a Jewish Iranian woman, approached a vast number of Israelis, in the hope that someone would be tempted to respond and ultimately recruited for purposes of intelligence gathering and terrorism, including against specific Israelis of interest to Iran. Initial contact was made through Facebook, ostensibly for business purposes. Thousands of people "friended" the fake profile, before being asked to move to WhatsApp. Targets were offered thousands of dollars, paid by Bitcoin, and in some cases subjected to romantic and emotional extortion.[103]

In 2020–2021, Charming Kittens conducted a phishing campaign against 25 senior US and Israeli experts specializing in genetic, neurological, and oncological research. The motives for the attack are unclear.[104] The motives for a phishing campaign in 2022 were clearer. This time Charming Kittens broke into the email accounts of a number of leading persons in Israel, whom they then impersonated in order to gain sensitive information from others. Among those impersonated were a former IDF general and former US ambassador to Israel. The "general" turned to former foreign minister Tzipi Livni, asking that she download and

comment on an article that he had ostensibly written. Livni spoke with the real general, confirmed that the article was a ruse and did not download the malware. Other targets included a senior official in a defense contractor and the heads of think tanks. In a number of cases, the hackers successfully gained access to private email exchanges, personal details of senior officials in sensitive defense firms, pictures of passports and classified documents. This information was used to continue the chain of impersonations.[105]

In 2021 the Agrius group launched a "password spraying" campaign against the Office 360 accounts of Israeli and US defense firms involved in the manufacture of satellites, drones, radar, and more. Twenty firms were successfully compromised.[106]

In 2022 Iranian hackers stole the identities of foreign and Israeli academics, journalists, reserve officers, businessmen and philanthropists, in order to lure them abroad and kidnap or cause them physical harm. A number of those targeted were on the verge of accepting an invitation to attend a fake academic conference. In another case, in which the attackers posed as Israelis of Russian descent, the targets were invited to meet with a real-life Russian billionaire's "assistant."[107]

CNI attacks—information operations have been a primary focus to date of Iran's overall cyber operations against Israel. As with the information operations Iran has conducted against the United States and other countries, the operations against Israel have been designed to foment internal divisions, counter Israel's positions on important issues, and promote support for Iran's overall deterrent posture.[108] Cyber information operations fit in well with Iran's ongoing efforts to isolate Israel and undermine its fundamental legitimacy as a state.

The Tel Aviv Times, a fake Iranian Hebrew-language website in operation since 2013 has 66,000 monthly views. The site carries articles plagiarized from mainstream Israeli news media with critical changes designed to support Iran's agenda.[109]

In 2014 Iranian-affiliated hackers temporarily gained control of the IDF blog and Twitter feed and sent out a message warning that the Dimona nuclear reactor had been struck by rocket fire and might explode. The IDF was able to restore control over the system fairly quickly, but in the interim many citizens feared the consequences.[110]

In 2016, even more ominously, an Iranian-affiliated website falsely quoted Defense Minister Moshe Yaalon as having said that if Pakistan sent troops to Syria to fight ISIS, Israel "would destroy them with a nuclear attack." The Pakistani Defense Minister responded by declaring that "Israel forgets (that) Pakistan is a nuclear state, too." Israel's Defense Ministry, concerned about a possible escalation with a hostile nuclear power, rapidly issued a statement clarifying that the story was a fabrication.[111]

In 2019 at least 350 fake accounts were found on Facebook, Twitter, and Telegram that were traceable to Countdown 2040, an Iranian website claiming that Israel will cease to exist by that year. Under the guise of ostensibly legitimate news websites, the fake accounts spread fictitious information to up to half a million people in Israel every month. Much like the Russian disinformation campaign against the US elections, Countdown 2040 often rephrases genuine news headlines in a manner designed to instigate divisive discourse on controversial issues in Israel, such as criticism of then Prime Minister Netanyahu, wealth inequality, sexual harassment, poverty, and the judicial system. The disinformation campaign was originally designed to inflame tensions over the Israeli-Palestinian conflict but was reset, following the announcement of early elections, in the attempt to influence the outcome.[112]

In 2019 the Harvard Belfer Center's website carried a report, attributed to the former head of the Mossad, Tamir Pardo, stating that Defense Minister Avigdor Lieberman had been dismissed after having been exposed as a Russian mole. Pardo had truly given a talk at the center, but the website had been cloned and the article was a complete fabrication, designed to sow discord in Israel. In reality, the Russian-born Lieberman had resigned over differences with Prime Minister Netanyahu regarding the situation in Gaza.[113]

In 2020–2021 an Iranian disinformation campaign sought to take advantage of the domestic political crisis in Israel at the time, to further amplify tensions and weaken it from within. Stolen identities of American Jewish philanthropists were used to gain information on the protest movement then underway against Prime Minister Netanyahu, and fake Facebook, Twitter, Instagram, and Telegram accounts disseminated inflammatory and violent messages designed to taint the movement. After Netanyahu was forced out of office, a Telegram account urged that he be imprisoned, sharing a photoshopped image of him behind bars. Telegram may have been chosen because, unlike other social media sites, it did not have mechanisms in place to prevent disinformation campaigns. Some experts believe that the techniques used were identical to those Russia had used during the US elections, suggesting possible collaboration.[114]

The Iranian campaign to foment domestic divisions and tensions continued in late 2021 and 2022. The Moses Staff hacking group posted the names, addresses, phone numbers, training, and roles of an entire IDF combat brigade. Aside from the severe security breach, the information included sensitive personal details, such as the soldiers' socio-economic status and mental health, including commanders' assessments that they suffered from "social or environmental deprivation," required close observation, or lacked a family support structure. A second dump, supposedly from the databases of the Israel Postal Authority and various private firms, included the personal details of hundreds of thousands of citizens.[115]

The cyber information campaign continued throughout 2022. The head of the Mossad's medical and dental records and ID card, along with a selfie taken at a sporting event in Tel Aviv, were leaked on Telegram, accompanied by taunting messages. The attack may have been an attempt to embarrass the Mossad and him personally, on the eve of an official visit to Washington dealing with the Iranian nuclear program.[116]

A cyber attack caused the air raid warning systems in Jerusalem, Eilat and Bet Shemesh to sound a false alert. The problem was rectified quickly, although presumably not without causing fear and even some panic among local residents, the attack's probable motivation.[117]

A personal Internet domain, which had belonged for 15 years to the editor of Haaretz, Israel's most prestigious newspaper, was purchased by unidentified sources when he no longer renewed a contract with the service provider. The hackers uploaded 200 articles that he had actually written onto the website, inserting three totally fabricated ones, as well. The three were designed to cause tensions in Israel's relations with Russia, following the outbreak of the war in Ukraine, Turkey, the Palestinians and possibly a Yemenite opposition group, fighting the Iran-backed Houthis. The three articles within also picked up by al-Manar, a Hezbollah affiliated website, as well as Greek, Turkish and Yemenite websites, for purposes of "circular amplification."[118]The above attack in which Charming Kittens impersonated an Israeli general and other senior officials (see section on CNE attacks), was also used to try and disrupt Israel's foreign relations. At the height of the war in Ukraine, the hackers sought to have an inflammatory billboard advertising campaign conducted in Israel against Russian President Putin. They also sought to harm Arab diplomats and businessmen posted in Israel, too disrupt Israel's relations with these countries.[119]

Combined attacks—mid 2020 marked the real turning point in the intensified Iranian-affiliated attacks mentioned in the CNA section. Many of the attacks now combined elements of disruption, espionage, and information operations as well as cyber crime, defying easy categorization. The primary intent may have been a psychological blow to Israel's sense of security and to its reputation.

Sapiens, an Israeli software firm, was forced to pay $250,000 in a Bitcoin ransomware attack after Iranian affiliated hackers threatened to shut down its system.[120] Tower Semiconductors paid several million dollars, rather than lose a single day of manufacturing time (worth approximately $3.4 million), after a ransomware attack damaged not just its information but operating systems, the "holy grail" of cyber attacks.[121] The attack against Tower may have been part of Operation Quicksand, a series of attacks against prominent Israeli firms conducted by Static Kitten, designed to look like ransomware but similar to the 2012 Shamoon attack that devastated Saudi Aramco's IT systems.[122]

Pay2Key, which is apparently affiliated with Fox Kittens, carried out a cutting-edge ransomware attack against seven Israeli firms, using their employees' remote connection systems. Four of the seven firms paid the ransom.[123] Black Shadow, another Iranian-affiliated group, hacked Shirbit, an insurance firm that caters for government employees, including those who work in sensitive defense agencies such as the ISA. This time, the attackers presented unrealistic deadlines for payment of a rapidly growing ransom and then dumped the stolen data on the Internet when the firm refused to pay. The data dumped included the names of those insured, the agencies they worked for, confidential hospital records, contents of WhatsApp conversations, home and email addresses, ID, phone, license plate and credit card numbers, and more.[124§]

The attack on Shirbit constituted a potentially unprecedented bonanza for intelligence services that might wish to spy on Israel's most sensitive agencies. It also demonstrated the poor cyber security typical of many firms in Israel, in this case even one subject to the ostensibly strict regulations of the ISA. The cyber security firm that Shirbit had hired, it subsequently transpired, employed someone who had only completed a brief training course, not a degree in information systems or computer science, and who only worked for the company part time.[125]

Amital, which provides specialized software to 70% of the logistics firms in Israel, was Pay2Key's next target. Once it had penetrated the firm's computer system, Pay2Key was able to spread to the systems of at least 40 of its clients and infect them with ransomware, putting much of Israel's air and maritime cargo traffic at risk. Some of the firms provide logistics services to the defense establishment, meaning that they have potentially sensitive information on the import and export of weapons systems. At least three firms were involved in the highly complex logistics surrounding the distribution of the coronavirus vaccine. The attack was discovered by chance, but rapid intervention by the INCD prevented further spread.[126]

Havana Labs, an Israeli subsidiary of Intel, lost to another attack by Pay2Key critical information regarding new semiconductors that were at the center of Intel's plans. The hackers also claimed to have penetrated the firm's domain controller, which would have given them access to its entire organizational network. Intel refused to pay the ransom and the sensitive proprietary information was released on the Darknet.[127]

Israel Aircraft Industries (IAI), a leading defense contractor and one of the most important firms in Israel, was also the focus of a major Pay2Key attack.

§ According to one source the attack against Shirbit was conducted by Hezbollah. Tal Shachaf, *YNet*, October 29, 2021.

In this case, the hackers posted the details of approximately 1,000 IAI system users, thereby indicating that they might also have gained access to sensitive information, such as the firm's anti-missile systems, drones, and precision guided munitions. By this point, Pay2Key had attacked over 80 Israeli firms, including a variety of defense industries.[128]

In 2021 Black Shadow was back with a Bitcoin ransomware attack against a car leasing firm, KLS Capital. As with the attack against Shirbit, the hackers' real motive was probably to demonstrate the weakness of Israel's defenses and cause it embarrassment. While negotiations were still underway, the hackers began a dump of personal data that dwarfed that of the Shirbit attack and also erased much of the firm's servers. Networm, likely just a new name for Pay2Key, conducted ransomware attacks against another Israeli logistics firm, Veritas, as well as against the Israeli franchise of the H&M clothing chain. Once again, the true objective appears to have been to embarrass and deter Israel. In this case Networm chose to impersonate a Russian attacker.[129]

In 2021 Black Shadow hacked the website of Israel's leading LGBTQ organization. The hackers initially demanded a large ransom but rapidly dumped the names of the nation's entire LGTBQ community on Telegram, along with explicit pictures, sexual preferences, chats, and health history, including HIV exposure. A parallel attack included the names of patients at a network of private clinics. Together, the two dumps included data on 1.5 million people.[130]

In 2022 an Iranian information campaign on multiple social media platforms, including Facebook and Telegram, posed as a Haredi (ultra-Orthodox) and nationalist Jewish group in Israel. Named Aduk, the Hebrew acronym for "virtual religious union for the religious community," the campaign sought to stoke internal division and inflame tensions with the Palestinians. Among other messages, it repeatedly called for attendance at antigovernment protests in Israel, particularly those organized by the far right; retweeted a call by an extremist Member of Knesset calling for "targeting killings" of Arab-Israeli "inciters," following sectarian tensions in Israel during the May 2021 conflict with Hamas; posted pictures falsely suggesting that the inclusion of an Islamist party in the coalition meant that Israel was controlled by Moslems; and encouraged anti-police sentiment among the ultra-Orthodox community. The attackers went to great lengths to make the website look genuine, creating a page for a fictitious bakery in an ultra-Orthodox town and in another case stealing the identity of an ultra-religious Jewish man who had died four years earlier.[131]

What Do All of the Attacks Actually Mean?

Israel is one of the primary targets of cyber attacks in the world today, by state actors, nonstate actors, hacktivist groups, and individuals. The barrage of attacks is nearly constant but has been found to increase significantly during periods of both heightened military hostilities and heightened diplomacy alike. Many of the attacks had neither a specific political agenda nor concrete demands and were part of broader campaigns against Israel.

Most of the attacks to date have been relatively unsophisticated, and Israel's defenses have usually succeeded in preventing significant damage, indeed, many are thwarted without the public even knowing of them.[132] The attacks have, however, clearly demonstrated that the threat is real and that the potential exists for significant disruption to Israel's critical national infrastructure, economy, military capabilities, international standing, domestic political discourse, and societal resilience. At least one attack, against the water supply, even demonstrated the potential for lethal harm. Most importantly, the number and especially the sophistication of the attacks is steadily increasing, whether for CNA, CNE, or CNI purposes, and the likelihood of more deleterious outcomes in the future is growing.

Experts remain divided about the sophistication of Iran's cyber capabilities, but there is no doubt that they have advanced significantly and will likely continue to do so, possibly with Russian and Chinese assistance. A similar process of continual improvement is demonstrably true of Hamas's more limited cyber capabilities. Starting from comparatively simple defacement and DDoS attacks a decade ago, both Iran and Hamas have launched considerably more sophisticated ones over time. Indeed, 2020 appears to have been a watershed year for Iranian attacks against Israel's civil sector. The publicly available evidence regarding Hezbollah is insufficient to substantiate a similar conclusion, but this most likely reflects the limitations of the information, not of its capabilities. Russia and China present growing threats in the cyber realm and the challenges are likely growing even from close allies, such as the United States and UK. Israel, in any event, has manifested growing concern, in both word and deed, regarding what it perceives to be a rapidly increasing threat.

The ability of Israel's adversaries to wage effective military cyber operations, as opposed to attacks on less well defended civil and commercial targets, remains unknown, at least from the public record, but appears to have grown significantly. Be that as it may, the cyber realm has provided Israel's adversaries, chiefly asymmetric actors such as Iran, Hezbollah, and Hamas, with an important new range of under-the-radar and deniable capabilities with which to offset Israel's conventional superiority. As in other areas of asymmetric conflict, they do not

seek to cause one or a few catastrophic cyber events, but to wage a long-term campaign designed to undermine Israel's national morale and societal resilience.

For Iran, cyber operations are not a stand-alone capability, but a complementary one, that buttresses other diplomatic, economic, and kinetic capabilities and can be employed in tandem with them. Although just a complementary capability, cyber has come to constitute a growing part of Iran's overall campaign against Israel. The same holds true of Hamas and presumably Hezbollah. In part, this may reflect a belief on their part that the cyber realm affords them an effective means of exerting ongoing pressure on Israel, with a comparatively low risk of retaliation and escalation. As will be seen in Chapter 10, Israel is, in fact, only known to have responded to cyber attacks, with cyber means, on isolated occasions and to have responded with kinetic means just twice, thereby lending credence to this assumption.

Attacks against Israel to date have further demonstrated the cyber realm's importance as an indirect means of achieving military objectives, without recourse to violence. Examples include the reported attacks against the IDF's civilian gas and food suppliers, whose activities can provide indications of military operations; attacks on private logistics firms, which may have exposed classified weapons exports and potentially caused disruptions to Israel's air and maritime cargo traffic; hacking of unencrypted live-feed from otherwise innocuous road cameras in order to improve rocket targeting and gain information regarding the location of IDF forces; hacking of IDF drones flying over Gaza in order to better hide Hamas rocket capabilities; or hacking of aircraft movements at Ben-Gurion airport for targeting purposes.

Israel's adversaries have conducted CNA attacks against critical national infrastructure as well as economic, governmental, and military networks. These attacks have yet to cause severely disruptive or destructive effects, but the potential was there, for example, in attacks on water, power, and communications installations or financial and military networks. The use of cyber for purposes of terrorist recruitment and perpetration of attacks already presents a real threat that may be growing.

The limitations of the public record, combined with the very nature of espionage, make it difficult to truly assess the effectiveness of the CNE attacks conducted against Israel to date. At a minimum, they appear to have been numerous and to have gained some classified information of significance. At least one, conducted by leading Israeli allies, the United States and UK, was actually severe.

CNE attacks have been conducted for various purposes. Some have sought to collect intelligence regarding Israeli defense industries, weapons development programs, and overall military capabilities, as well as Israel's nuclear policy

and strategic thinking generally. Others have been conducted in preparation for future rounds of conflict with Hamas or Hezbollah, to steal intellectual property, whether from Israeli defense firms or coronavirus researchers, and to gain insights into Israel's scientific and technological capabilities. Israel's extraordinarily high smartphone penetration rate, second in the world according to one study,[133] including many of Chinese provenance, has been an important vehicle for CNE attacks.

The treasure trove of intelligence that Iran and others stood to gain from the attacks on Shirbit and KLS Capital may have been the Israeli equivalent of the severe damage by the United States in the Russian SolarWinds attack, of which Israel was also a victim. In the case of Shirbit and KLS, the damage was further compounded by the subsequent Iranian decision to dump the stolen data on the web as part of an information campaign designed to embarrass Israel. The United States and UK have presumably conducted other effective CNE operations against Israel and most likely Russia and China as well.

CNI attacks have been extensive. Some have caused financial and reputational damage regarding the effectiveness of Israel's cyber capabilities, such as the series of attacks against Israeli firms in 2019–2021, or sought to undermine its international standing, such as the attacks on the broadcast of the Eurovision Song Contest and aircraft bringing global leaders to attend an Auschwitz commemoration. Other attacks have been used to try to cause potentially severe escalations with foreign nations, even at the nuclear level in the case of Pakistan, or to sow panic in Israel itself, for example, the attack that claimed that the Dimona reactor had been hit by a rocket and might explode. Still others have sought to create and further exacerbate domestic divisions and discord, affect electoral processes, and undermine Israel's societal resilience. None of the CNI attacks against Israel to date have approached the comprehensiveness and sophistication of those conducted against the US elections and their actual effectiveness has been limited. Nevertheless, there is deep concern in Israel over the potential for harm.

Devastating effects at a systemic national level have yet to be demonstrated against Israel, but not for lack of intent. The capabilities of Israel's adversaries are improving steadily, and the law of averages is against Israel. Sooner or later, a devastating attack will happen, whether in peace time or during a major military confrontation, should Israel's adversaries choose to withhold their truly sophisticated capabilities until that time. The potential for significant and in some cases even severe damage has already been demonstrated, and there is every reason to believe that it will grow in the future.

For now, Israel maintains clear cyber superiority over all regional actors, but it faces multiple adversaries who are constantly at work to improve their capabilities. If the basis for an assessment of the threat is limited to the number of successful attacks that have taken place to date and the actual consequences

they have caused, the cyber threat to Israel has been significant, but limited. If, conversely, the assessment is based on a realistic assessment of the potential for disruption and damage, the threat is already severe. Moreover, as is true of the challenges in other realms, Israel's adversaries may only have to cause devastating damage once, whereas its defenses must be successful 100% of the time.

The defenses that Israel has put in place to address the cyber threat and the counter measures it has taken are presented separately in the following chapters. When viewed in isolation, without knowledge thereof, the cyber threat to Israel is frightening. It remains frightening enough even when viewed in combination with the defense strategy. Either way, Israel's response to the cyber threat reflected overwhelming strategic necessity.

PART III

A NAPKIN THAT CHANGED HISTORY

Israel's Cyber Response

In Part II we addressed the first half of the hypothesis presented in the Introduction, which held that the causal variable of strategic necessity explains the development of Israel's advanced cyber capabilities, the dependent variable. Part III addresses the second half of the hypothesis, which added the variables of socioeconomic necessity and opportunity to the causal relationship. Both parts of the hypothesis were in accordance with the realist school of international relations theory.

We further posited that strategic culture was an intervening variable that shaped Israel's perception of the options available to it and consequent decision to adopt a technological response to the challenges posed by its environment. Indeed, advanced technological capabilities had long been considered a primary engine of socioeconomic growth and source of the qualitative military edge with which Israel would counter its adversaries' quantitative superiority. By the 1990s, when cyber first emerged, Israel had already become a global center of high tech, and cyber was particularly suited to its innovative national culture and self-identity. As such, Israel's response to the cyber realm also reflected domestic cultural factors, in line with the constructivist school.

Part III begins by presenting an overview of Israel's strategic culture (Chapter 6), for background purposes, before turning to four chapters, each of which presents a different dimension of the dependent

variable: the cabinet decisions that formed the basis for Israel's civil cyber strategy and the strategy's outlines (chapter 7); Israel's remarkable cyber ecosystem and innovative cyber culture (Chapter 8); international cyber cooperation and law (Chapter 9); and Israel's military cyber strategy and the primary offensive cyber operations attributed to it (Chapter 10).

6

Strategic Culture and National Security Strategy

A country that sees itself living on the tip of a volcano, or inside the eerie halls of Yad Vashem,[*] does not plan for the future and does not think about bold initiatives. It only holds on for dear life.

Tom Friedman, former *New York Times* correspondent in Israel

Chapter 6 addresses two critical and interrelated issues. It begins with an overview of Israel's strategic culture, the intervening variable presented in the Introduction, and of its national security strategy. It then turns to a brief analysis of Israel's national security decision-making processes, including some of the primary failings and strengths thereof. The discussion of these issues is designed to place the ensuing chapters, on Israel's response to the cyber challenge, in a broader perspective and to see how they influenced the choices Israel made in this regard.

Israel's Strategic Culture

A nation's strategic culture, in keeping with the ideas of the constructivist school of international relations, is deeply rooted in its historical beliefs, collective memories, values, traditions, mentality, and the assumptions it holds regarding its strategic circumstances. States' self-identified needs, culture, and goals do not directly determine their policies but do have an important influence on them.

To understand Israel's strategic culture is to appreciate an historic mindset. Israel does not view itself as just another state among many but as the culmination of a long, rich, and often bitter history and of a 2,000-year-old dream

[*] Israel's national Holocaust memorial.

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0007

of national redemption. The Jewish people's long history of persecution, culminating in the Holocaust, imbued Israel's national psyche with a fundamental sense of insecurity. For two millennia, life in the diaspora was an ongoing struggle for survival, and the fear of extermination, as demonstrated by the Holocaust, was not an abstract notion but very real. "The nineteen centuries from Masada to Maidanek"—respectively, the heroic scene of the final collapse of the Jewish rebellion against Rome in 73AD and of one of the infamous Nazi concentration camps—weigh heavily on Israel's leaders, public, and foreign policy.[1] In reality, Israel's historical memory goes back much further, to the early Biblical era and destruction of the First Temple, and continues to be written to this day, with the searing experiences of the contemporary dispute with the Arab countries and Iran, terrorism, and international opprobrium.

Israel's encirclement by enemies openly avowed to its destruction, with far greater populations and, at least in the early decades, resources and military power, magnified the historic sense of insecurity and led to the basic Israeli assumption that the nation faces an ongoing existential threat. The resulting "siege mentality," "Masada complex," or "Holocaust syndrome," various characterizations attached to Israel, reflect this primal fear and consequent national preoccupation with survival and security, which are the foremost factors shaping Israel's identify and driving its strategic culture and national security policy.

Defense Minister Dayan's infamous warning, during the bleak early days of the Yom Kippur War, regarding the possible "end of the Third Temple" (i.e., Israel's destruction), is one of the more extreme expressions of this primal fear, but it has been manifested often, even when the dangers were far more circumscribed or distant. "Our fate in the land of Israel," Prime Minister Begin intoned, "is that we have no choice but to fight with selfless dedication. The alternative is Auschwitz."[2] Mossad Director Meir Dagan warned during the 2006 Lebanon war that Israel's existence would be threatened if it failed to win.[3] Prime Minister Netanyahu repeatedly drew comparisons between Germany in 1938 and Iran today.[4] Syria, Hezbollah, and Hamas are also presumed to seek Israel's destruction.

Holocaust Remembrance Day is a poignant annual reminder of the dangers the nation continues to face. Countless offices are decorated with a famous picture of Israeli F-15s flying over Auschwitz, an incomparable visual encapsulation of the dramatic transformation that took place in the fortunes of the Jewish people in just a few decades. Each year, on Passover, virtually all of Israel's Jewish population recites the centuries-old warning that "in every generation they have risen-up against us to annihilate us," a theme that continues to resonate strongly with much of modern-day Israel.

Numerous states throughout history have faced a threat of politicide (destruction of the state); Israel is unique in that its leaders and people believe that it also faces a realistic threat of genocide and national extinction. The dangers posed by Israel's external environment are thus considered to bear little substantive comparison to other countries.[5] Israel's experience has further demonstrated that national security decisions may fundamentally transform the nation's course, even when they do not threaten its destruction, as happened following the Six-Day War and the Oslo agreement.[6]

From the beginning, Israel's leaders believed that the conflict would last for decades or even centuries and that the various wars and lower-level hostilities were all mere stages in one long confrontation.[7] To this day, many in Israel view the ongoing conflict with the Palestinians as a continuation of the War of Independence in 1948.

Arab enmity was believed to be so unremitting and deeply held that merely thwarting their efforts to destroy Israel would not be sufficient to achieve deterrence. Israel's actions could affect the Arabs' cost-benefit calculus but not their fundamental enmity, and it was destined to live under a protracted existential threat. Israel could not afford to lose a single battle, let alone a war. If defeated once, it would never have a "second chance" and its wars were thus existential "wars of no choice."[8] A corollary of the sense of national vulnerability is the exaggerated reaction to any sign of friendship, or estrangement, from other countries. All countries experience ups and downs in their foreign relations; for Israel they are personal and visceral.

The preoccupation with security gave rise to the preeminent role played by the IDF and defense establishment in Israeli society. The IDF is not just another national military, whose sacrifices accord it the reverence common to militaries in many countries, but a unique embodiment of national rebirth and the guarantor of the nation's existence.

Israel is the only Jewish and Zionist state among the numerous Christian, Moslem, and other nations of the world. For the most part, Israel pursues a statist foreign policy, similar to other nations, in which the raison d'état is preeminent, but its unique character has a significant effect on its strategic culture and national security policy. Israel was explicitly established to be the nation-state of the Jewish people, indeed, this remains its national raison d'être, and maintaining and securing its existence, as such, is the overriding objective of Israeli national security policy. For Israelis and many diaspora Jews, Israel is "special" in ways that cannot be fully expressed in words, and they are caught up in a great historic enterprise of rebuilding a unique new-old state and assuring the future of the Jewish people.[9]

Despite the overwhelmingly pragmatic nature of Israeli national security decision-making and policy, it does, at times, also display strong elements of

ideology and faith. In some historical situations, it has been argued, careful and rational planning can actually be counter-productive, leading to self-doubt, self-defeating prophesies, and paralysis, whereas unwavering adherence to national dreams, to an "unattainable future," can help make them possible. At times, especially during the early decades, when considerations of pragmatism might have counseled caution, Israel's leaders had to make leaps of faith based on the force of will, an historic sense of destiny, and a willingness to take the risks necessary to overcome objective assessments of Israel's capabilities.[10]

A precarious balance between hard-headed realism and ideology has thus long been a basic hallmark of Israel's strategic culture and national security policy. The entire Zionist project, Israel's very establishment against all odds, was based on will, a degree of ideological romanticism, and a sense of destiny, which overcame pragmatic considerations of relative power.[11] Israeli lore celebrates the spirit of "can do" leaders and officers (*bitsuistim*) who press forward without regard for constraints. Indeed, Israel itself is perceived as the victory of the determined few over insurmountable odds. The national ethos celebrates the famous statement by Theodore Herzl, the founder of modern Zionism, "if you will it, it is no dream," while many are familiar with the story of Ben-Gurion's decision to declare independence, over the fears of many "experts" and fellow ministers. Israel's spectacular successes in the early years further reinforced this sense that determined leaders could achieve almost anything, such as tripling the national population, building national housing, economic, and scientific infrastructure, and the dramatic military victory of the Six Day War.[12] Israel has matured, and issues have become far more complex and difficult to address, yet Israel's belief in its ability to overcome the nearly insurmountable, remains largely unshaken.

The exceptions to the essentially pragmatic approach, since the state's establishment, have been few. Most have had to do with the future of the West Bank, which is a matter not just of territory and security for Israel but of fundamental beliefs regarding the nature of the state and the aims of Judaism and Zionism.

Surrounded by hostile Arab states on all sides, Israel has long seen itself as a state under siege, and its geography as a strategic nightmare. Indeed, the borders, especially the pre-1967 ones, were considered essentially indefensible and an invitation to attack by their very nature. Israel feared attacks not just by the bordering Arab countries but by a coalition including those in the "second tier," such as Iraq and Saudi Arabia. The defense doctrine even took into account the worst-case scenario, termed the complete case, in which the Arab countries succeeded in banding together and jointly surprising Israel.[13]

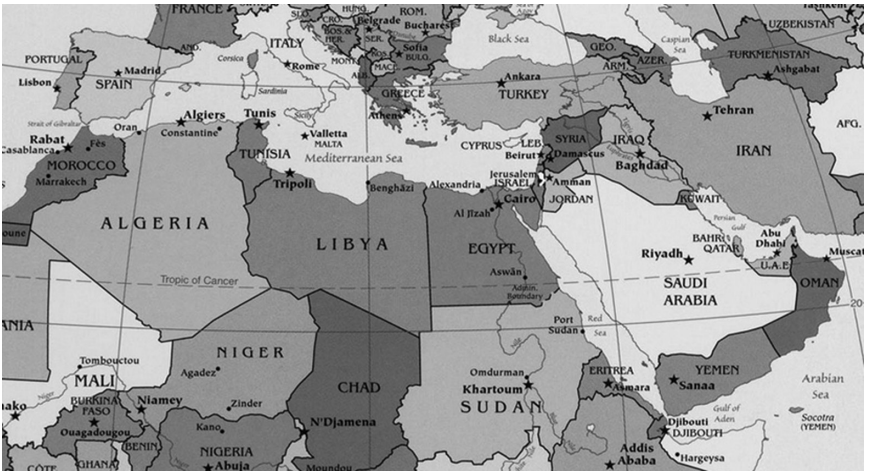
As seen in Map 6.1, Israel is tiny, slightly over 7,700 miles^2 (20,000 km^2) within its 1967 borders, approximately the size of New Jersey or Slovenia, and approximately 9,600 square miles (25,000 km^2) including the West Bank and Golan Heights. Moreover, its borders are narrow and highly elongated, meaning

Map 6.1 Israel (1967 Borders)

that Israel could be overrun at a number of points. From north to south Israel measures just under 300 miles. Its width varies, being just 80 miles at the widest in the Beersheba region, with three particularly narrow points: the so-called "finger" of the Galilee in the north, where Israel is approximately 5 miles wide; the "narrow waist" at Netanya, just 20 miles north of Tel Aviv, the very heart of the country, where it is 8.7 miles wide; and the southern tip below Eilat, where the V-shape ends in a narrow point.

Virtually everything that makes Israel a viable state is concentrated in the narrow coastal plain, primarily in the area between Haifa and Ashkelon, a strip about 100 miles long and 10–15 miles wide in most areas (the one significant exception, Beersheba, is an isolated enclave in the south). Most of the population and economic base, approximately 70% and 80% respectively, are located in this area, as are most governmental institutions, the international airport, airbases and other strategic targets, national infrastructure, academia, and the arts. All are within easy artillery, let alone rocket, range from the West Bank and other borders. Armored forces deployed in the West Bank would literally abut Jerusalem and be just minutes from Tel Aviv. Flying time for combat aircraft based in any of the neighboring countries would also be measured in minutes.

One merely has to look at Map 6.2 to understand the fundamental territorial asymmetry that animates Israel's fears, whether one includes the entire Arab world or just what was once termed the "confrontation states" (Egypt, Jordan, and Syria). Egypt alone is 50 times Israel's size, Jordan almost five times, Syria nine. Saudi Arabia is the size of all of Western Europe; the other Arab states are of various sizes, but most are far larger than Israel. Israel could never conquer the Arab states, but the opposite was not the case. More fundamentally, Israel's



Map 6.2 The Middle East in Context

minute territorial dimensions, along with the fear that the population in any territory conquered, even temporarily, would be annihilated, meant that it could not conduct a tactical, let alone a strategic, withdrawal. It also means that most of its population continues to be vulnerable, in many cases even to light arms.[14]

The balance of power between Israel and the Arab countries is believed to be characterized by a number of fundamental asymmetries, in terms of geography, population, economic resources, diplomatic backing, and war aims. Some of these asymmetries are immutable, others have changed dramatically over time, largely in Israel's favor.

Israel's population has always been tiny compared to the Arab world, with two primary consequences. The Arabs, it was long believed, had infinitely greater reserves of manpower to draw upon, and their tolerance for pain, ability to suffer losses, and consequent staying power would thus be far greater.[15] The Arab side was also able to draw upon far greater economic resources, a critical component of national power, which provides them with the ability to purchase more weapons and sustain larger militaries than Israel. The explosion in Arab petrowealth starting in the 1970s further magnified this fundamental asymmetry.

These asymmetries were further believed to mean that Israel would lack the staying power required for protracted confrontations and that it could not afford to mobilize the reserves for long, because this would paralyze the economy.[16] Add to this, Israel's sensitivity to casualties, and a serious problem of staying power was thought to exist. In practice, Israel's rapidly growing economy, together with US assistance, has enabled it to maintain a far larger standing army than thought possible, although Israel still does have a problem of economic staying power when forced to mobilize the reserves. Its societal staying power has also proven stronger than many believed likely.

The Arab side, furthermore, began every dispute with Israel with the relatively unanimous support of the entire Arab and Moslem world, a large starting coalition. This basic Arab advantage was further augmented by strong support from many Third World states and often even from Western ones.[17] The great powers were also believed to pose a major constraint on Israel's defense doctrine and freedom of action. The United States forced Israel to withdraw from Sinai in 1949 and again in 1956. Along with the other leading global powers, it has long put pressure on Israel to make a variety of concessions, territorial and otherwise, in negotiations with the Palestinians and Arab states. The United States pressed Israel not to preempt in 1967 and 1973 and together with the Soviet Union prevented clear victories in the War of Attrition in 1970 and Yom Kippur War in 1973. The great powers, it was feared, might also intervene directly on behalf of the Arabs, as the Soviet Union threatened to do in 1973, before Israel had succeeded in achieving its military objectives, or worse, after the Arabs had

achieved some of theirs. Israel could win the wars, but the great powers might deprive it of victory, and it would lose the diplomatic battle.

Given the overall asymmetries between the sides, Israel further believed that it would be unable to terminate the conflict with the Arab side through military means, compel them to accept its existence, or generally translate its military achievements into political successes. The tremendous disparity in size and resources would further sustain Arab hopes of future success and both intra and inter-Arab politics would perpetuate the conflict.[18] Israel's war objectives have thus been essentially defensive in nature, to maintain the status quo by thwarting Arab attempts to destroy it, and defined mostly in military terms. The important diplomatic progress of recent decades, including the peace with Egypt and Jordan and the Abraham Accords, has only partly mitigated the perception of overwhelming Arab hostility.

Israel's Response

Given this harsh strategic reality, it was believed that Israel could never match the quantitative economic, military, and diplomatic imbalance with its Arab adversaries. Israel could, however, better mobilize all of the human and material resources available to it, through nearly universal military conscription of both men and women and better training, command and control, resourcefulness, and motivation of its forces. It also meant a particular emphasis on technology, both for direct military purposes and to build the socioeconomic basis needed to sustain the defense effort.[19]

Israel recognized from the beginning that it would be highly dependent on the outside world for diplomatic, economic, and military support. When coupled with its fundamental sense of insecurity, this produced an ongoing preoccupation with the need to secure at least one major power patron. The lesson to be learned from Jewish and Israeli history, however, was that foreign patrons were not fully reliable,[20] a fear that was realized in practice with the French arms embargo of 1967. Even the United States, a remarkable benefactor, has not always been a reliable guarantor of Israel's security. In 1981, after extensive bilateral exchanges made it clear that the United States would not end the threat posed by Iraq's then-active nuclear program, Israel concluded that it had no alternative but to act independently and bomb the reactor. A similar situation prevailed in 2007, leading Israel to once again take independent action and destroy a Syrian reactor then under construction. Other nuclear and non-nuclear examples also exist.

The importance of the relationship with the United States for Israel's national security cannot be overstated, nevertheless. Washington is usually the first and often even sole port of call for strategic consultations on emerging events, almost

always the foremost one, and inevitably the primary means of addressing them. Indeed, the relationship with the United States has become a fundamental component of Israel's overall national security strategy, and its very survival today is at least partly dependent on it.

The importance of the relationship goes way beyond the monetary value of US military assistance. The United States is committed, by congressional legislation, to the preservation of Israel's qualitative military edge, that is, its ability to defend itself, by itself, against all regional enemies. The United States and Israel engage in an extensive, almost unparalleled, process of strategic dialogue and joint planning at all levels, from the president and premier down. Military cooperation includes rocket and missile defense, bilateral and multilateral exercises, pre-positioning of US equipment and weapons in Israel, homeland security cooperation, and more. No less important is the diplomatic cover that the United States provides Israel in the UN and a plethora of international forums, in the face of an endless array of injurious resolutions regarding the peace process and Palestinians, various Israeli military and diplomatic initiatives, and, of particular note, its purported nuclear capabilities. Israel probably also enjoys a de facto US security guarantee, should its existence be threatened.[21]

Along with the overriding importance that Israel has attached to the maintenance of a major power patron, and in partial contradistinction, its strategic culture has placed at least as great an emphasis on the principle of strategic autonomy, or self-reliance, that is, the will and capacity to take independent action to defend itself, even in the face of opposition from major powers, including the patron. Patrons may be relied on to help maintain the balance of power and deterrence between wars but not to come to Israel's direct aid, and, in any event, alliances are temporary, subject to various considerations and constraints, and ultimately fleeting. In the end, Israel will always remain a "nation dwelling alone" and only it can bear responsibility for its defense. Israel would thus ask its patrons for the means with which to defend itself, but not for troops or direct guarantees.[22] The principle of self-reliance has also meant that Israel would aim to develop both a technology-based economy and indigenous weapons manufacturing capability.

Technological prowess has been a fundamental pillar of Israel's strategic culture and socioeconomic policy from the earliest days, even before the state was established. As a small and resource-poor country, facing an existential threat, it was believed that Israel could only survive and ultimately thrive by developing the highly advanced technological capabilities necessary to promote rapid economic growth. A rapidly growing economy, in turn, would create the requisite basis for the development of the qualitative military edge with which Israel sought to counter Arab quantitative superiority.

To these ends, massive investments in education, science, and technology were essential. Over time, Israel became a world leader in both civil and military high tech, known informally, if perhaps with some hyperbole, as the "startup nation."[23] The cyber realm, in particular, with its emphasis on outstanding scientific and technological creativity and innovation and its potential for rapid and high returns on investments of a comparatively modest scale, was considered particularly suited to Israel's national strengths.

Diplomacy and foreign relations are a further component of Israel's national security response. Given Israel's strategic exigencies, defense considerations have long eclipsed almost all others and foreign policy has been viewed primarily as a subordinate tool for achieving them. During the early decades, the overarching objective of Israeli foreign policy was to ensure a stable source of weapons, an objective that was largely achieved in the 1980s with the institutionalization of the military relationship with the United States. Together with the peace agreements with Egypt and Jordan, new opportunities for diplomacy and foreign relations emerged and Israel has relations today with more countries than ever before. In 2020 the Abraham Accords ushered in a new era, in which Israel also has formal relations with the UAE, Bahrain, and Morocco, as well as informal but growing ties with a variety of Arab states, most importantly Saudi Arabia. In addition to a unique relationship with the United States, Israel also enjoys good-to-strong bilateral relations with essentially all of the major global powers, including Russia, China, India, the UK, France, Germany, Japan, and more.

Israel's military doctrine has long been based on three primary pillars, known as the 3Ds: deterrence, detection (early warning), and decisive defeat. Starting in the mid-2000s, a fourth D, defense, was added.

Deterrence—the defense doctrine was predicated on the assumption that Israel could not achieve its political objectives through the use of military force, and deterrence thus became its centerpiece.[24] Israeli thinking differentiated between four types of deterrence: *current deterrence*, focused on low-intensity conflict, primarily terrorism; *specific deterrence*, to prevent major military operations, especially surprise attacks, by establishing "red lines" and casus belli whose violation would elicit an Israeli response; *strategic deterrence*, designed to prevent a general or large-scale war; and *cumulative deterrence*. The latter was designed not just to dissuade an adversary from realizing its hostile intentions in the near term but more fundamentally, to convince it that its efforts to destroy Israel would be defeated every time it sought to do so and were thus futile, thereby diminishing its motivation to try to begin with. Cumulative deterrence was to be achieved through both limited military confrontations and large-scale wars.[25] In the long term, it was hoped, cumulative deterrence would ultimately lead the Arab states to accept its existence, as has happened, in practice, with many.

Detection—that is, timely and precise early warning, is expected to alert Israel to impending failures of deterrence and provide sufficient time to mobilize and deploy the reserves. The Arab standing armies' ability to rapidly shift from defensive to offensive operations, Israel's primarily reservist military and its lack of strategic depth, all imbued the concept of detection with a place of special importance in its strategic thinking.[26]

Defeat—of an enemy is commonly defined as the ability to prevent an enemy from continuing to wage a conflict, by either destroying its military capabilities or undermining its psychological will to do so. In Israel's case, conversely, Arab hostility was believed to be so fundamental that the most it could realistically aspire to was a temporary respite between recurrent rounds of warfare, not defeat in the classic sense of ending the conflict. Israel's deterrence would fail every few years, renewed hostilities would break out, and partial defeat of the enemy would restore deterrence and the lull between rounds. Each round, however, was to end with a sufficiently decisive outcome to provide for the long-term cumulative deterrence Israel sought.

For Israel, the concepts of deterrence and defeat were two parts of a synergistic whole: defeat of the enemy would restore deterrence, deterrence would limit the need for further defeat.[27] The combined deterrence-defeat concept proved successful with Egypt and Jordan, which ultimately despaired of achieving their objectives by military means and pursued a diplomatic resolution to the conflict, and in later years contributed to Israel's formal recognition by the UAE, Bahrain, and Morocco and informal acceptance by others. It also proved sufficient to bring the Syrians and Palestinians into advanced, if ultimately unsuccessful, negotiations in the 1990s and early 2000s.

Israel's military strategy distinguishes today between limited operations, such as those in Lebanon and Gaza since 2006, and full-scale wars. In the former, the strategy merely seeks to remedy the proximate causes of conflicts and rapidly return to the status quo ante, without trying to achieve broader strategic objectives, such as an enemy's defeat and a change in the overall situation. In cases of war, in contrast, the strategy seeks to defeat the enemy and affect a strategic change in the situation, from the outset.[28]

Israel's strategic culture is fundamentally defensive, to ensure the survival of the state, but operationally offensive. Only offensive and mobile maneuver warfare would enable Israel to determine the timing, tempo, and location of the battle, bring its qualitative advantage to bear, and achieve the decisive outcomes needed to promote cumulative deterrence. In the early decades, this offensive approach was translated into the belief that Israel must transfer the fighting to enemy territory as rapidly as possible and that it must end with the IDF in control of more territory than it had started with.

Offensive mobile warfare was also considered critical in order to keep conflicts as short as possible. The longer a conflict lasted, the greater the danger that additional actors would join the fighting; the risks to regional instability and global oil supply would increase, as would the blow to Israel's economy. Lengthy conflicts would also increase the need to petition a foreign patron for emergency resupply and the probability of adverse superpower intervention. This latter factor gave rise to the possibly unique Israeli concept of political time, the period Israel would have to conduct military operations before external intervention forced a cease fire on unfavorable terms.

Defense—Starting in the 1990s, the nature of the military threats Israel faces changed, from primarily state-based conventional threats from standing Arab armies to asymmetric conflicts with Iran, Hezbollah, and Hamas, in which Israel's home front has become the primary battleground. The changing nature of the threat led to a reassessment of the role of defensive operations in Israel's strategic culture and to the adoption of a new, fourth D, defense.[29] The difficulties that Israel has encountered in recent decades in maintaining those territories already under its control, let alone expansion to new ones, further reinforced this change in approach and led to a preference for standoff combat, primarily from the air, without recourse to territorial conquest.

Over the years Israel has built a large military capability designed to cope with the conventional military threats it faced. In recent years, IDF modernization programs have shifted to the capabilities it will need to counter the threats posed by Iran, primarily its missile and potential nuclear capabilities, and the rocket arsenals of Hezbollah and Hamas.[30]

Counterterrorism—as a form of asymmetric warfare, similar in some respects to the cyber threat, Israel's counterterrorism (CT) policy is a source of particular interest for our purposes. The policy has long been predicated on a fundamental assumption, that terrorism could never be fully defeated just minimized and reduced to a level that Israel's society could tolerate.[31]

Israel's CT policy has applied a combination of deterrence, offensive, and defensive measures along with international cooperation. Offensive measures have included ongoing CT operations, often round-the-clock, ranging from small covert operations to major offenses, attrition warfare designed to grind down terrorist organizations, interdiction of arms transfers, targeted killings of senior operatives, the occasional spectacular CT operation, and more. An especially important Israeli innovation, at least partially adapted for cyber defense as well, is the "intelligence-operations circle." This highly honed coordinating mechanism, developed during the second *Intifada*, enables Israel to transfer intelligence regarding impending terrorist attacks to the operational units (air and/or ground forces) and turn it into actionable interdiction measures within minutes.[32]

Defensive measures have included fences along the borders, security zones extending beyond the border, border patrols, and more. In the case of the West Bank and Gaza, Israel has also sought at times to use economic growth as a means of creating a Palestinian stake in stability and hopefully leading to a reduction in terrorism.[33] International cooperation has ranged from informal, ad hoc measures to more formal agreements, including intelligence sharing, operational coordination, and training.

Israel's CT policy has produced a variety of outcomes, some highly successful others failed and even counterproductive. Overall, it has been a major success, reducing the threat to a level that Israel's society can tolerate and even thrive in, especially economically.[34] Conversely, terrorism has had a major impact on public opinion, greatly influencing and even swaying a number of electoral outcomes, hardening public attitudes toward the Palestinians and even affecting Israel's positions in negotiations with them. Some of Israel's CT measures have also had a highly deleterious impact on its international standing.

To address the more contemporary terrorist threat, stemming from rockets directed primarily against its civil home front, Israel has built a multi-tiered offensive and defensive response. Offensively, Israel has developed a partial capability to destroy rocket and missile launchers through the application of massive and precise air power.[35] Defensively, Israel has deployed a number of anti-rocket defensive systems, of which Iron Dome is the best known, in addition to passive defenses, such as shelters and reinforced concrete rooms in private dwellings. These measures have proven highly effective in minimizing casualties and reducing public pressure on Israel's leaders to preempt, counterattack immediately, or launch major ground operations, thereby affording them greater decision-making latitude. The sense of security has also greatly reduced the public's sense of helplessness and strengthened its long-term resilience and ability to withstand the continuing threat.[36]

Nevertheless, the rocket threat continues to pose enormous operational challenges, greatly exacerbated by the fact that Hezbollah and Hamas intentionally embed them among the civilian population and/or hide them in underground tunnels, thereby making the task of finding and destroying them extremely difficult. Even a partial mitigation of the rocket threat, as demonstrated in the repeated rounds with Hamas and Hezbollah since 2006, can require weeks of fighting, during which Israel's civilian population remains under continual attack.

All of the major rounds with Hezbollah and Hamas since the 1990s have been "deterrence-based operations," designed to prevent further attacks and restore calm, weaken the two groups significantly, and deter a renewal of hostilities for as long as possible, that is, to force a return to the status quo ante, without specifying how long it was expected to last. In the long term, Israel hoped that

these repeated deterrence-based operations would achieve a level of cumulative deterrence and result in a cessation of the attacks, but it had no pretensions to fully resolving the problem in the short term.[37]

In effect, Israel was seeking to counter Hezbollah's and Hamas's long-term strategy of defeating it by means of attrition warfare, with a new attrition strategy of its own. Part of the "campaign between the wars" (MABAM), Israel's strategy was designed to strengthen its deterrence between the major rounds and dissuade its adversaries from beginning further attacks for as long as possible. Since they could not, in practice, be defeated in one major operation, it was necessary to repeatedly "mow the grass."[38] These conflicts have become so continuous that the campaign between the wars has in many ways become the primary campaign, rather than a distinct concept.

The IDF has not been able to fully achieve its objectives in any of the major rounds with Hezbollah and Hamas, all of which have ended with a sense of frustration, especially since Israel enjoys both quantitative and qualitative superiority in these conflicts. The difficulties that the IDF has encountered present Israel with a fundamental quandary. As painful as the threats posed by Hezbollah and Hamas are, Israel does not want to conduct a ground invasion to occupy Lebanon or Gaza, probably the only effective way of rooting the rockets out and greatly reducing the threat, and possibly even to dislodge the two groups. The reluctance to do so does not stem from an inability to achieve these goals but from the price to be paid and the belief that Hezbollah and Hamas will rebuild their rocket arsenals once Israel withdraws and that the respite gained will actually be brief. Moreover, if Israel does dislodge either Hezbollah or Hamas, the resulting power vacuum may be filled by even more dangerous organizations, such as ISIS. The bottom line is that Israel does not yet appear to have an effective offensive response to the Hamas and Hezbollah threats, is not likely to have one for the foreseeable future, and is thus placing far more emphasis on defense than in the past.[39]

Iran—Israel's defense establishment is divided regarding the best means of addressing the Iranian nuclear threat. Some are said to believe that an Israeli attack on the Iranian nuclear program could achieve a delay of at least a few years, which is not insignificant in and of itself but might also destabilize the Iranian regime. Moreover, an Israeli strike might force the international community to become actively engaged, even militarily, to prevent the program's renewal. Those who favor this approach apparently believe that Israel's existing retaliatory capabilities are sufficient to deter Iran and that it should thus focus on strengthening its offensive ones.[40]

Others are more skeptical and reportedly believe that the delay achieved by an Israeli attack would not justify the costs and thus that attempts to develop an effective offensive capability are an ineffective use of precious resources. Those

who favor this approach consequently place greater emphasis on deterrence, including greater investment in Israel's retaliatory capabilities and the hardening of critical strategic sites against nuclear attack.[41] Some, in both camps, harbor a hope, not always discreetly, that the United States will resolve the problem, diplomatically if possible, militarily if necessary.[42]

In the meantime, Israel has reportedly conducted hundreds of strikes in Syria in the attempt to prevent Iran from turning it into a forward operating base against Israel for both itself and Hezbollah, as well as for transferring advanced weapons to Hezbollah in Lebanon. There are also reports of Israeli attacks against Iranian capabilities in Iraq and Yemen. Given the mammoth rocket arsenal that Iran has provided Hezbollah, and the major developments that have taken place in Israel's counter capabilities, a balance of power, or maybe balance of terror is a better term, has evolved along the border and both Israel and Hezbollah are mutually deterred.

Nuclear ambiguity[43]—Israel has a carefully thought out policy of nuclear ambiguity, according to which it neither acknowledges nor denies having nuclear weapons or in any other way indicates what its nuclear strategy might be. Indeed, its public posture in this regard is limited to an intentionally opaque stock statement that "Israel will not be the first country to introduce nuclear weapons into the Middle East." In practice, Israel is thought to have been a nuclear power since approximately 1970 and to have a robust arsenal based on a nuclear triad (missile, air, and submarine-based platforms).

Israel's purported nuclear capabilities are commonly considered a "doomsday option," one that might be used only in extremis, if the nation's existence was threatened, and which is thus essentially irrelevant to all lesser scenarios. Based on understandings reportedly reached with the United States over five decades ago and concerns about both the regional and international ramifications of a possible decision to divulge its capabilities, Israel has strictly adhered to the policy of nuclear ambiguity.

The nuclear strategy also has a preventive component, the so-called Begin Doctrine, according to which Israel will prevent any hostile state in the region from acquiring a military nuclear capability. The doctrine has been successfully implemented on two occasions to date, with Israel's bombing of the Iraqi and Syrian nuclear reactors in 1981 and 2007, respectively. The Begin Doctrine may, however, have now run its course. In the early 2010s, at a time when both the premier and defense minister were reportedly considering a military strike against Iran's program, the IDF chief of staff, head of Mossad, and other defense chiefs were apparently strongly opposed, especially if conducted without US approval.[44]

Whether for that reason or not, the Begin Doctrine has not been implemented so far against Iran, at least in the classic sense of an air strike, although the numerous

kinetic and cyber attacks that Israel has reportedly conducted to sabotage, delay, and derail Iran's nuclear program may be a new means of implementing it. Some reports have referred to targeted killings of Iranian nuclear scientists, others to explosions at Iranian nuclear and missile sites. The Stuxnet virus, reportedly a joint US-Israeli covert cyber attack, which led to the destruction of Iranian nuclear centrifuges and to the postponement of the Iranian program[45] is the most famous of these efforts.

The preventive strategy also has a strong diplomatic component. The heart of this has been an intensive, decades-long, diplomatic and PR effort, designed to inform leading international actors and their publics of Arab and Iranian WMD programs and to convince them of the threat they posed not only to Israel but also to international security. Facing an international community that has often been deeply unattuned to issues of WMD proliferation, an important part of the effort has simply been the provision of intelligence regarding the status of the various programs and analyses of the intentions behind them. Israel's efforts successfully contributed to the US decision to impose unilateral sanctions on Iran as early as 1996 and later to the imposition of international sanctions in 2012. Israel's earlier role in regard to the Iraqi nuclear program was similar, if less significant.

Israel is threatened by WMD more than any other state in the region and thus views regional WMD disarmament, including a Middle Eastern WMD free zone, as a "coveted end-state."[46] Israel believes however, that it cannot join global nonproliferation regimes at a time when other regional states are still in a state of war or refuse to negotiate with it, or refuse even to consider measures needed to ensure ongoing stability and coexistence. Moreover, Israel argues that what is needed is agreement not just on nuclear disarmament, an area in which the Arab side believes that it holds the advantage but also on comprehensive WMD and ballistic missile disarmament, thereby bringing Iranian and Arab WMD programs into play as well.[47]

Arms control agreements have repeatedly failed to prevent states in the Middle East from developing WMD programs, even though they were signatories to them. Indeed, four of the five violations of the Nonproliferation Treaty (NPT) to date were committed by Middle Eastern states (Iraq, Iran, Syria, and Libya), who knowingly undermined arms control agreements by systematically cheating, for example, signing the NPT and then developing nuclear weapons programs. Some states in the region have also used chemical weapons, including Syria, Egypt, and Iraq, a signatory to the Chemical Weapons Convention. For reasons of verifiability, Israel is therefore deeply concerned about the feasibility and effectiveness of global nonproliferation regimes in the Middle East and believes that they do not constitute an adequate response to the threats it faces.[48] Instead, it supports the adoption of special regional disarmament arrangements,

with more robust verification regimes. Arms control under this approach would be the final result of an incremental process designed to transform the security situation in the region and lead to peace and normalization, rather than being the first step and a precondition, as demanded by the Arab side.[49]

A final component of Israel's unconventional response is defense. Missile defense is of limited efficacy, however, against nuclear missiles. If just one nuclear missile got through, it would constitute a catastrophic failure that would negate the defensive system's potentially great success in shooting down all of the rest.[50]

National Security Decision-Making in Israel

Surprisingly, perhaps, for a nation so overwhelmingly preoccupied with foreign and defense affairs, Israel has yet to formulate an official national security strategy or even a defense doctrine. Israel does not issue the equivalent of US National Security Strategies or Quadrennial Defense Reviews, UK-style White Papers, or other comparable strategic statements.[51]

Founding Prime Minister David Ben-Gurion was Israel's only leader to formulate a defense doctrine while in office. The Ben-Gurion Doctrine, formulated in the 1950s, remains the closest thing Israel has to a national security strategy to this day, but was neither fully elucidated in writing nor officially adopted. In the decades since, a number of attempts have been made to update the doctrine and adapt it to the dramatic changes that have taken place in Israel's strategic circumstances; all have failed to either reach fruition or be formally adopted.

The failure of Israel to adopt a national security strategy is an important issue in its own right and a reflection of the country's overall approach toward national security policymaking.[52] In recent years a dramatically transformed Middle Eastern landscape, the difficulties that Israel has encountered in the conduct of military operations, and a growing sense among practitioners and scholars alike that something was amiss in Israel's national security praxis has led to renewed interest in fundamental strategic thinking.

In 2006, a major interagency strategic review (the Meridor Committee) was widely hailed for its depth, and in practice the IDF has partially implemented its recommendations, even though they were never approved by the cabinet. In 2015, for the first time ever, the IDF issued a formal statement of national military policy, the IDF Strategy, in both classified and non-classified versions, later updated in 2018. Although an important departure from all previous IDF practice, the IDF Strategy did not constitute an overall defense doctrine, certainly not a national security strategy, and explicitly called for the formulation of such higher-level strategic statements. In the mid-2010s, the National Security Staff (NSS) conducted basic policy reviews of Israel's military and counterterrorism

strategies and even completed a draft national security strategy, which was subsequently stymied by bureaucratic warfare.[53] A number of important academic and think tank studies have also been published.[†]

The absence of formal policy statements does not mean that considerable strategic thinking does not take place within Israel's national security establishment or that numerous policy papers are not generated. They are. They tend, however, to be issue-specific and ad hoc.

Primary Determinants of the Decision-Making Processes

Israel's national security decision-making processes are shaped by three primary factors: its external environment, its electoral system, and the primacy of its defense establishment.

The External Environment—ever since its establishment, Israel has faced a uniquely harsh external environment. Repeated wars, major confrontations, and ongoing threats, from terrorism to massive rocket attacks and WMD programs, diplomatic warfare, isolation, and delegitimization, have all kept national security at the forefront of Israeli life. Each war and, at least in the past, every battle, was viewed as one of survival, part of a threat of national extinction, with a consequent need for constant vigilance.

A small nation, a virtual city-state by international standards, Israel's national security environment is far more complex than that of most states, indeed, the national security challenges it faces, diplomatic, military, economic, and technological, are more appropriate to those of a major power. Israel's external environment is further characterized by extraordinary volatility, extreme both in the breadth and frequency of change and in the consequent level of uncertainty. It can be said, with only some hyperbole, that crisis is the expected steady state in Israel.

The environment has further proven to be particularly difficult to shape, thereby circumscribing the options available to Israel and its latitude to make decisions in the national security realm. The infamous "three nos" of the 1967

[†] Shelah (2015) addressed the primary defense and military challenges Israel faced at the time, primarily regarding Hezbollah and Hamas. Arad et al. (2017) presented a broad-stroke, grand strategy for Israel, focusing largely on societal, economic, and technological issues. Dekel and Einav (2017) offered an interesting, but unfortunately brief proposal for a new national security concept. Freilich (2018) presented the most comprehensive proposal to date for an overall Israeli national security strategy. Former Chief of Staff Eisenkot and Siboni (2019) presented a briefer proposal of this kind the following year.

Arab League summit in Khartoum—no negotiations, no peace, and no recognition of Israel's right to exist—enshrined in both symbolic and practical terms the belief that Israel faced an essentially monolithic wall of Arab enmity. It also meant that Israel was unable to use repeated military victories to dictate the terms of the peace. Dramatic peace proposals to the Palestinians and Syria[‡] similarly failed to yield commensurate diplomatic breakthroughs. In these circumstances, Israeli decision makers largely accepted their inability to foresee and shape Israel's external relations. Some adopted an at least partially reactive approach to decision-making, others were remarkably proactive, nevertheless.

In recent decades, starting with the peace agreements with Egypt and Jordan and culminating in the establishment of relations with the UAE, Bahrain, and Morocco, the sense of nearly unremitting Arab and Moslem enmity has been punctuated by periods of dramatic diplomatic breakthroughs. Changes in the regional balance of power and consequent Arab strategic considerations, largely in response to the rise of Iran, have now yielded the promise of heretofore unimaginable areas of collaboration in both the military and civil realms. The enmity of Iran, Hezbollah, and Hamas toward Israel is believed to be fundamental and immutable, but Israel's ability to shape its external environment has clearly grown greatly.

The Electoral System—Israel's proportional representation electoral system is extraordinarily representative, providing virtually all currents of public opinion with a voice in the Knesset, but also resulting in the need to govern through coalition governments. Almost from the moment elections end and a new government is formed, coalition preservation and maintenance become a nearly all-consuming preoccupation for the premier, often superseding all other considerations. The mechanics of coalition maintenance, including the imperative for compromise to achieve at least some minimal working consensus, turn the cabinet into a forum for ironing out differences between its component parties, or obfuscating them, rather than serving as a true policymaking body. The result is a clear tendency toward procrastination and sub-optimal solutions, often inaction, as leaders wait for issues to reach the point where they have no choice but to make some decision.

Israeli political life remains unusually intense, especially in comparison with other Western democracies. Partly the result of Israel's severe external environment, as well as deep public divides over a number of fundamental domestic and foreign issues, policy is typically debated in highly ideological and partisan terms. Politics thus exert a significant and often untoward impact on

[‡] Prime Minister Barak's proposal to the Palestinians at Camp David and under the Clinton Parameters in 2000, and Prime Minister Olmert's proposal to them in 2008; Prime Minister Barak's proposal to the Syrians, presented by President Clinton at the Geneva summit in 2000.

the decision-making process (DMP), foreclosing some options in advance, channeling others in given directions. With short terms between elections, often only 2–3 years, and a frenetic 24/7 news cycle, both premiers and ministers are consumed with the need to jockey for position, pander to their party constituencies, and ensure their political futures. Political success is often tied more to intra-party politics than effective policy and governance.

As in other parliamentary systems, the premier is neither commander-in-chief nor chief executive, as in the US presidential system, and requires cabinet approval for virtually all decisions, including the use of force. In fact, an Israeli premier's formal prerogatives of office are particularly circumscribed, even when compared to other parliamentary systems. The premier's ability to lead is thus essentially a function of his or her basic political skills and actual political power at any given moment. Those premiers who have been in firm control of their parties and coalitions have proven to be effective and powerful leaders, capable of promoting ambitious political agendas. Those who were not, have found that their limited formal sources of authority left them at the mercy of the contending political forces.

Ministers are appointed on the basis of their own and their party's political clout, not their professional expertise in their ministerial portfolios, nor their managerial experience, giving rise to misgivings regarding their competence to deal with the issues at hand, especially considering the short time most serve in their cabinet positions. There is also a basic structural question, whether one needs the minister of agriculture, for example, in a meeting dealing with national security or the ministers of defense and foreign affairs in meetings on agricultural matters. Moreover, the cabinet's size has become unmanageable, precluding the conduct of effective and discreet deliberations, and meetings tend to consist largely of political grandstanding rather than substantive policy formulation.

Given the minimal political consensus that holds coalitions together, the cabinet tends to become a conglomerate of semi-autonomous ministerial fiefdoms, rather than an integrated and collective decision-making body. Once ministers have devoted the time and resources necessary to formulate a preferred policy option, they are loath to reopen an issue in a large and politicized body such as the cabinet, or the subcabinet Ministerial Committee on Defense (MCoD), and tend to view meetings as an ordeal to be endured, rather than a venue for serious policy deliberation. Policy proposals are usually presented by the premier or relevant minister, that is, the primary policy advocates, who invariably present one favored position that the cabinet can either accept or reject. Although the NSS does often propose alternative policy options, they are generally not the subject of a systematic attempt by the cabinet to assess the differing courses of action.

The politicized nature of the DMP, premier's limited statutory authority, dysfunctions of the cabinet, and exigencies of coalition politics, including the constant danger of leaks, all dictate the political wisdom of avoiding clearly

defined policy objectives and of maintaining constructive ambiguity. In practice, Israel's political leaders have refrained from conducting systematic policymaking processes, apparently because they are incompatible with their political needs. In a highly politicized coalition system, premiers do not wish to be bound by formal processes requiring that they present the cabinet with a systematic analysis of their objectives and the alternative policy options for achieving them. Strategic clarity amplifies differences, both substantive and political, and can put political futures at risk. Ambiguity, conversely, can often be crucial to a premier's ability to hold a fractious coalition together and thus be constructive. As a result, Israel's premiers have long manifested a predilection for either avoiding systematic policymaking processes or limiting them to narrowly focused issues.

Premiers tend to formulate policy either on their own, in informal groupings of a number of ministers ("kitchen cabinets"), or in even smaller ad hoc forums consisting of only those few senior office holders with whom they have no choice but to consult (e.g., the defense minister, Chief of Staff, and intelligence chiefs) and possibly one or two trusted and respected ministers or senior advisors. These informal and ad hoc forums, unlike the MCoD and cabinet plenum, do provide for effective and discreet policy deliberation, and their recommendations often carry considerable weight. They do not, however, have the statutory authority to make decisions, and their recommendations must be formally approved either by the MCoD or cabinet plenum. The increasingly important role of the NSS has strengthened the premier's policymaking capabilities and contributed somewhat to the quality of cabinet deliberations, but Israel still does not have an effective *statutory* decision-making forum.

On many issues, including those of major importance, Israel simply does not have formal policies beyond the personal preferences of the premier and other senior ministers, and issues tend to be dealt with in an "atomistic" fashion, rather than as part of an overall strategy. Major policy outcomes are thus typically the cumulative and even unintended product of a series of ad hoc solutions to immediate needs. Continual improvisation and crisis management, rather than forethought, planning, and deliberately chosen courses of action, are the primary means by which Israel makes policy. This basic tendency is further reinforced by the rapid rate of coalition turnover, which forces decision-makers to focus on the immediate electoral ramifications of their actions. The result is a national security DMP geared overwhelmingly toward the resolution of concrete and immediate problems, rather than long-term governance.

As the issues facing Israel have become increasingly complex and the national security bureaucracy has grown in size, the need for more effective inter-agency coordination has assumed greater urgency. A common problem of governments everywhere, it is further exacerbated in Israel by the informal nature of decision-making, fear of leaks, and politicization.

Primacy of the Defense Establishment—given the harsh circumstances of Israel's birth and the decades of hostility ever since, the defense establishment has long enjoyed a disproportionate share of national resources and influence. From the outset, resources have been concentrated primarily within the IDF and intelligence agencies, whereas the Ministry of Defense (MoD) and especially the Ministry of Foreign Affairs (MFA) were accorded far more circumscribed roles.

The IDF is the single most influential player in the national DMP. No other institution can compete with the ability of the IDF's intelligence, planning, and operations branches to generate rapid and sophisticated policy assessment, planning, and implementation capabilities, round the clock. The IDF's institutionalized role in the DMP, as well as the high accessibility afforded by the small size of the political and military elites and the close personal ties between them, add to its influence.

The IDF is further perceived as the primary representative of the national collective, a strictly professional, non-partisan, and trustworthy actor around whose positions the warring factions in the coalition can coalesce. Once the IDF has taken a position, it is easier for political leaders to adapt their positions accordingly, and they use IDF assessments and recommendations to legitimize political positions. IDF positions do not dictate the nature of cabinet debate and decisions but do wield enormous influence. In most cases, the IDF's positions are Israel's national security policy.

Strengths of the Israeli National Security DMP

Its dysfunctions notwithstanding, Israel's national security DMP does have a number of strengths. The uninstitutionalized, informal, and often improvisational nature of the DMP is one of its primary ills, but also has important advantages. Given the extraordinarily frenetic character of Israel's external environment, the ability to improvise, change gears, and rapidly adapt to changing circumstances is a vital necessity. Time and again, Israel has been forced to adapt to unexpected, sweeping changes in its external environment that have forced it to regroup, rethink its basic strategy, and gear up for new challenges. Moreover, in a politically charged society, improvisation vitiates the need to formulate clearly articulated objectives and priorities and thus suits the political needs of the premier and other ministers. Israel overdoes it, improvising when it is neither necessary nor appropriate, but the ability to do so is critical and has become a national sphere of excellence and virtual faith.

Although decision-making at the cabinet level is often highly charged politically and dysfunctional, the national security establishment takes a practical, problem-solving approach, and its DMP is highly structured and systematic. In

practice, when stripped of its surface rhetoric, dynamic and pragmatic decision-making is also characteristic of much of the political leadership. In the face of necessity or opportunity, Israeli leaders have repeatedly demonstrated the ability to revise existing policies, even those based on long and deeply held convictions and strategic outlooks.

The boundaries between Israel's civil and military institutions are highly porous and the national security establishment is comparatively small, thereby facilitating a common understanding of the issues and creating a high level of personal and professional intimacy. Perhaps most importantly, the porous boundaries enable easy and rapid communication that cuts through organizations and levels of bureaucracy.

As in other countries, Israel's national security establishment engages in bureaucratic wars for turf, prestige, and influence. The severity of the threats Israel faces does, however, force a modicum of discipline on the system, and senior officials and ministers have often known each other for years. Together, this has helped mitigate the bureaucratic battles and generally kept them from reaching some of the extremes found in other countries.

Israel's judiciary intervenes in decisions made by the IDF and other government agencies to a far greater extent than virtually any other in the world, thereby setting limits to what can and cannot be done. Israel is analyzed and often skewered both by the domestic and international media, thereby providing an immediate means of gauging reactions to policy. The various parts of the national security establishment are in continual contact with the international community, at all levels and in almost all areas—politico-military, diplomatic, scientific, and otherwise—exposing them to an ongoing exchange of ideas, feedback, and constraints. Exchanges with friendly governments serve as an important input into the Israeli DMP and a "reality check." Information and policy exchanges with the United States are so extensive that US policymaking capabilities almost become an extension of Israel's. Short-term difficulties aside, the Israeli national security establishment's exposure to this external system of normative, media, and professional scrutiny also has advantages and can be a source of strength.

The national security establishment, as a whole, is highly professional but has a number of centers of particular excellence, including the intelligence community, Israel Air Force (IAF), and various sophisticated and high-technology units. Moreover, the dysfunctions of the national DMP are at least partly overcome by the quality and experience of the people involved.

In conclusion, many observers fail to understand how a regional power with highly advanced conventional military capabilities, commonly thought to be a nuclear state, can continue to harbor such deep-seated existential fears. Nevertheless, Israel's strategic culture cannot be understood without

comprehending this primal fear of annihilation, a perceptual prism through which all issues of importance are viewed, and its never-ending, consequent quest for greater security. Even today, seven and a half decades after Israel's independence, the fundamental sense of insecurity is so deeply imbued that neither all of its military victories nor, probably, any level of military might could ever alleviate it. Israel's haphazard national security decision-making processes are also part of the picture. In the ensuing chapters we will see how both Israel's strategic culture and its decision-making processes played out in its efforts to address the opportunities and dangers posed by the cyber realm.

7

The Civil Cyber Strategy

(Cyber) is one of the greatest challenges facing humanity . . . It is an ever-present race . . . We need to run ahead and stay ahead . . . This is a supreme test for our civilization . . . .

Prime Minister Netanyahu

The defensive shield . . . will not be one system, but a combination of several systems that will enable us to be in a much better place . . . you need something at the state level and this state level becomes the digital equivalent of the Iron Dome.

Prof. Eviatar Matania, former Head of Israel's National Cyber Directorate

The first part of the hypothesis presented in the Introduction posited that Israel's cyber capabilities were developed primarily in response to the emergence of a new and dangerous external threat. As such, they were held to constitute a strategic imperative, reflective of the realist school of international relations theory. To substantiate the hypothesis and place the Israeli case in a broader perspective, Chapter 1 presented the global cyber threat and the dangers it poses, while Chapters 4 and 5 presented the cyber threat that Israel itself has faced to date.

In this chapter we begin our discussion of how Israel has responded to the cyber threat, starting with the civil strategy it formulated and the institutional arrangements it put in place to implement it. As further posited in the Introduction, we will see that domestic and bureaucratic politics played a role and influenced some of the decisions made.

The chapter has four sections. We begin with a series of decisions adopted by the cabinet between 2002 and 2015. Together, they essentially constitute Israel's cyber strategy. The second section on the National Cyber Security Strategy issued by the INCD in 2017 presents an overall conceptual statement of the strategic thinking behind the cabinet decisions. The third section presents some of the actual measures adopted by the INCD to defend the civil cyber realm. The

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0008

final section presents an assessment of the INCD's effectiveness some five years after it began operations.

The Cabinet Decisions and Institutional Framework

In the 1990s, Israel was among the first states to identify the dramatic threats and opportunities embodied in the then nascent information revolution, including the disruptive effects that growing computing power, personal computers, and the Internet were already having on commercial, governmental, and defense organizations. This changing perception was part of the broader change then underway in Israel's strategic landscape, from state-based conventional threats to asymmetric ones, aimed primarily at its home front, such as terrorism, rockets, and now cyber, by state and nonstate actors alike. It was also part of Israel's long-standing focus on technology as the solution to both its economic and defense needs. The defense establishment helped impress the importance of the changing strategic environment on the national leadership and provided much of the necessary knowledge, especially in the technologically complex area of cyber.[1]

The various government ministries and agencies began their first forays at that time into e-governance, web services, Internet connectivity, and cyber security, leading in 1997 to the establishment of *TEHILA*,* one of the first governmental cyber security bodies in the world and the basis for the far more advanced gov.il e-government portal now in use. *TEHILA* was tasked with promoting greater integration between the different agencies responsible for Israel's information systems, ensuring a more secure and unified governmental IT structure, including secure Internet access and hosting of government websites and e-government services. In so doing, it was also to generate greater governmental efficiency and budgetary savings.[2]

In 1998 the Knesset passed Israel's first major cyber legislation, the Law for Regulating Security in Public Institutions, which delineated the areas of responsibility of the different agencies involved. The Israel Security Agency (ISA, aka Shin Bet, Israel's domestic intelligence service), was designated the lead agency for civil cyber security, including responsibility for protection of critical national infrastructure, the primary focus of concern at the time. ISA's designation as the lead, rather than a civilian agency, together with the IDF's responsibility for the military cyber realm, clearly reflected Israel's defense-driven priorities.[3]

* A Hebrew acronym for Government Infrastructure for the Internet Age.

Nonetheless, Israel's early response to the emerging cyber threat was generally uncoordinated and erratic, with each agency essentially conducting its own independent efforts. In 2002 the cabinet thus instructed the NSS to conduct a policy review regarding Israel's policies in the cyber realm. The result was Cabinet Decision B/84,[4] which remains the fundamental basis for much of Israel's cyber strategy to this day.

Cabinet Decision B/84: "Responsibility for Protecting Computer Systems in Israel"—adopted in 2002, this was one of the world's first national cyber security policies. The decision set out general guidelines for the protection of critical national infrastructure and also established two special bodies. The first, a Steering Committee chaired by the NSS, was tasked with conducting an overall assessment of the cyber threat Israel faced; determining which public and private computer systems were critical to its security and would thus be placed on the Critical Infrastructure List; formulating policies, standards, and operating procedures for their protection; promotion of cyber R&D; and determining the various agencies' areas of responsibility. The second, a new National Information Security Authority (NISA, or RE'EM, in the Hebrew acronym), was to be responsible for cyber regulation of public and private sector organizations and for protecting organizations on the Critical Infrastructure List. It was also to provide professional guidance to the IDF, intelligence services, and other agencies that would continue to bear responsibility for the defense of their own computer systems.[5]

In a harbinger of the more severe bureaucratic warfare that would emerge later, the means by which the NISA was to actually carry out its responsibilities and which agency to place it in came to be among the main issues considered by the Steering Committee. The ISA's responsibility for civil cyber defense up to that time raised difficult questions of democratic governance and civil liberties. Moreover, the ISA, IDF, and police were only allowed to intervene in public and private sector cyber matters for very specific security-related purposes and subject to stringent legal controls, meaning that their ability to defend the civil cyber realm was limited.[6] A number of models were thus considered, including a laissez-faire approach, which left civil cyber security entirely to market forces; a public-private partnership; delegation of authority to the police, with a focus on crime prevention; delegation of authority to the defense organizations; and establishment of an entirely new agency for critical infrastructure protection.[7]

In the end, the Steering Committee preferred to play it safe and decided to place the NISA within the ISA, despite these difficulties, and on the organizational basis of an already existing information security unit. Establishment of an entirely new bureaucratic entity would have required a lengthy and difficult legislative process in the Knesset, whereas the ISA already had the necessary expertise, and an amendment of existing legislation was all that was needed.

Time was a critical factor during a period in which Israel was almost completely preoccupied with the second Intifada.[8]

Unsurprisingly, the NISA ran into opposition from the beginning, especially from the public and private entities it was tasked with regulating. The high costs involved in implementing the regulations it promulgated, as well as issues of civil liberties, privacy, and transparency were the primary foci of criticism. The Tel Aviv Stock Exchange (TASE), in particular, put up a fight, arguing that it was already well aware of the threats in the cyber realm, had the requisite expertise to deal with them, and, in any event, already adhered voluntarily to the most advanced international cyber security standards, thereby obviating the need for formal oversight. Most of all, the TASE argued that oversight by an intelligence agency might cause investors to fear for their privacy and tarnish not only its own reputation beyond repair but also that of Israel's financial sector as a whole, resulting in a potentially massive flight of capital. It took until 2008 to reach a compromise, and it was only then that TASE finally agreed to come under NISA oversight. In hindsight, the catastrophic results it feared never materialized,[9] but they did feed into the later decision to establish the INCD as an independent organization, separate from the intelligence community.

By 2010 the continually growing cyber threat, including the attacks on Estonia and Georgia (see Chapter 2), had spurred renewed concern regarding the effectiveness of Israel's response up to that time to the threats that it faced. Whereas the government and defense establishment had made considerable progress in defending their computer systems, the public and private sectors had not, despite Decision B/84 and the establishment of the NISA.

During a visit to Unit 8200, Israel's signals intelligence agency, Prime Minister Netanyahu was clearly excited to learn of the developments in the cyber realm. On the way to his next meeting, the premier drew a triangle on a napkin, illustrating the primary dimensions of what would become the basis for Israel's national cyber strategy. At the top of the triangle were the government and IDF, who would be responsible for defending Israel's civil and military cyber realms. At the base of the triangle were cyber industry and academia, which were to provide the basis for the development of Israel's cyber capabilities and turn it into one of the world's leading cyber powers. Netanyahu gave the napkin to his military secretary and told him to "take care of it." In the absence of more explicit instructions, the latter took the premier's words to mean that he had been charged with turning the vision set out on the napkin into concrete action.[10]

In this somewhat haphazard manner, not atypical of its improvisational decision-making processes, was Israel's national cyber strategy born. In concrete terms, the result was a decision to establish a National Cybernetic Task Force, charged with formulating an overall national approach to the cyber realm, to

guarantee Israel's security and achieve global leadership in the field. To this end, the task force was to recommend ways of developing a new cyber ecosystem, as well as the technological infrastructure and institutional arrangements best suited to Israel's needs. It was headed by Major General (ret.) Professor Isaac Ben-Israel, a highly respected expert in the area of technological innovation and a former head of the R&D Directorate in the Ministry of Defense.

The task force found that the cyber threat to Israel had grown significantly in the years since Decision B/84, despite the measures that had been taken. Governmental and defense bodies had put cyber security measures in place, the needs of critical national infrastructure systems had been addressed, and the police were dealing with cyber crime. The vast majority of the population, however, including small businesses, some government services, and private individuals remained insufficiently defended, with no one to turn to for their cyber security needs.

The task force's recommendations, formally submitted in 2011, became the National Cyber Initiative. Arguably the two most important recommendations were that Israel seek to become one of the top five cyber powers in the world by 2015 and, to this end, that it establish a single body to formulate and coordinate all national cyber policy, the new Israel National Cyber Bureau (INCB), the precursor of today's INCD. To develop an advanced cyber ecosystem, the National Cyber Initiative further recommended that cyber education begin in elementary school, interdisciplinary academic cyber programs be established in the universities, and the government work to develop the cyber security industry in partnership with the private sector. The basic idea was to create a self-perpetuating cycle: academic research was to generate scientific knowledge, which would be used to develop new technologies and commercial applications with high added value; the defense establishment would benefit from the knowledge and capabilities created, further spur academic research and commercial applications on the basis of its own needs, and provide some of the outstanding personnel needed; and the entire cycle would be continually repeated. The National Cyber Initiative further recommended, unsurprisingly, that Israel strengthen its military cyber capabilities.[11]

Cabinet Decision 3611: Promoting National Capacity in the Cybernetic Space—the recommendations of the task force were turned into official policy and, in effect, into a national strategy by Cabinet Decision 3611, adopted in 2011. The decision set out four primary objectives: to turn Israel into one of the top five global cyber powers; develop its national cyber capabilities and ability to address future cyber challenges; improve protection of the national infrastructure and of computer systems and networks in Israel generally; and promote cooperation between academia, the private sector, government, and the defense establishment.[12]

To this end, the INCB was now formally established and made directly subordinate to the prime minister. The INCB was charged with formulating and implementing a comprehensive national cyber strategy to replace the approach adopted a decade earlier by Decision B/84, including promotion of cyber R&D, industry, education, regulation, and international cooperation through promotion and assistance with coordination; formulation of an integrated national cyber assessment based on the different intelligence agencies' assessments; and taking responsibility for protecting government ministries and critical national infrastructure, with the exception of the telecommunications sector, which remained under the ISA. To this end, Decision 3611 also provided for the transfer of the NISA from ISA to the INCB. In recognition of the bureaucratic strife likely to result, the decision stressed the need to further delineate the various agencies' areas of responsibility and called for the establishment of a dispute resolution mechanism.[†13]

Ongoing bureaucratic turf wars reached new heights in 2014, necessitating intervention by the prime minister and establishment of a new interagency task force. The ISA, the agency most adversely affected by the establishment of the INCB, had questioned the need for a separate cyber agency from the beginning and remained strongly opposed to the transfer of responsibility for protection of the critical national infrastructure to the INCB under Decision 3611.

Drawing on its extensive and highly successful experience in counterterrorism, and the overall offensive approach embodied in Israel's strategic culture, the ISA stressed the need for proactive operations to prevent cyber attacks before they occurred, rather than post-facto responses, and argued that the INCB lacked both the intelligence gathering capabilities and ties with counterparts abroad necessary to do this effectively. The ISA further maintained that the changing threat required that the NISA be transferred back to it and that the mandatory information sharing procedures it had put in place with parts of the civil cyber realm be further expanded. The INCB countered that the ISA's approach would exacerbate the already existing tensions between security needs and privacy rights and stressed the importance of having a civilian agency bear responsibility for protecting the public and private sectors, including critical infrastructure. To this end, the INCB proposed that the ISA bear responsibility for countering attacks and the attackers themselves, while the INCB would provide protection to the organizations under attack.[14]

[†] Decision 3611 also formalized the Israeli definition of the term cyber realm as: "The physical and nonphysical space, that is created, or comprised of all or part of the following: mechanical and computer systems, computer and communications networks, software, computer information, content transferred by computerized means, traffic and monitoring data and users of all the above."

Cabinet Decisions 2443 and 2444—in 2015 the cabinet adopted two new decisions: Decision 2443 Promoting National Regulation and Governmental Leadership in Cyber Security and Decision 2444 Promoting National Preparedness for Cyber Security.

Decision 2443 provided for the establishment of a multi-tiered national regulatory framework designed to "systematically and consistently" improve the robustness and resilience of Israel's civil cyber realm. The new regulatory framework was to be based on the empowerment of the existing regulatory agencies, rather than establishment of new ones, adoption of best international practices, and differentiation between the levels of protection required by different actors. It also provided for the appointment of a cyber steering committee in each ministry and agency, chaired by the director general,[‡] and for an organizational cyber director. To implement the decision, each ministry and agency was to allocate no less than 8% of its annual information technology budget during the first two years, 6% in some cases, to be increased thereafter.[15]

Decision 2443 further provided for the establishment of a new Governmental Unit for Cyber Defense (GUCD), to provide government agencies with professional guidance regarding the cyber realm and help them prepare organizational defense plans. The GUCD was to be subordinate to the Governmental Telecoms Authority but operate under the professional guidance of the INCD, with which it was to jointly operate a national Computer Emergency Response Team (CERT-IL) and Security Operations Center (SOC) responsible for cyber security incident management.[16]

Decision 2444 constituted an operational strategy designed to centralize all national efforts in the civil cyber security realm. To this end, it provided for the establishment of a National Cyber Security Authority (NCSA), which would operate alongside the INCB. Together, they would form the new INCD, a single bureaucratic entity responsible for all areas of civil cyber security.[17] The INCB would continue to bear responsibility for formulating Israel's cyber strategy and policies, national capacity building, and promotion of its standing as a world leader in the cyber realm. The NCSA, in contrast, was to be an operational agency responsible for providing a "comprehensive and continuous response" to public and private sector cyber security needs, including: civil cyber intelligence collection and early warning; ongoing assessment of the national cyber situation; promotion of national cyber resilience; development of human resources and cyber R&D; guiding the private and public sectors on responses to attacks; guidance and oversight for regulatory agencies; and protection of civil liberties

[‡] The senior official in each government ministry or agency, directly subordinate to the minister.

in the cyber area. The NCSA was also to chair an interagency steering committee to better coordinate efforts.[18]

Although Decision 2444 explicitly stated that the ISA's authority in the cyber realm was not to be adversely affected, it actually constituted a final rejection of the ISA's approach and sealed the INCD's preeminence in public and private sector cyber security. Two related sets of considerations tipped the bureaucratic battle in the INCD's favor: the need to better balance security and economic concerns and a growing appreciation that in a democracy, only a civilian entity, not a counterintelligence agency, could bear responsibility for public and private sector cyber security.[19] Considerations such as these also informed the decision to refrain from assigning a law-enforcement role to the NCSA, unlike most other cybersecurity agencies around the world.[20] In practice, there may have also been a third and more prosaic reason for the INCD's bureaucratic victory; the other agencies did not initially believe that the INCD would become a player of significance.[21] Be that as it may, the ISA and INCD signed an MoU in 2016, which led to some improvement in interagency cooperation.[22]

Cabinet Decision 3270—the INCD began operating just over a year after Decision 2444 was adopted. The decision did not, however, sufficiently define the hierarchical relationship between the INCB and NCSA, thereby setting the scene for continued bureaucratic friction. The issue was resolved in 2017 by Decision 3270, which provided for the full integration of two entities under the INCD. The INCD's direct subordination to the prime minister reflected the great importance that Israel attached to the cyber realm. Only three other defense-related agencies share this exclusive status, the Mossad, ISA, and Atomic Energy Committee,[23] all of which bear responsibility for similarly critical and sensitive areas.

In 2016 the aforementioned Law for Regulating Security in Public Institutions, Israel's first major cyber legislation from 1998, was revised considerably, to provide post-facto statutory authority for some of the changes made in practice under Cabinet Decision 2444. Prominent among these changes were the transfer of responsibility for protecting critical infrastructure from the ISA to the INCD and the requirement that every government agency appoint a cyber security director. The revised law still did not define what "critical infrastructure" constituted and thus which systems were to be placed under INCD guidance, other than to state that they were those so designated by the agencies authorized to do so.[24]

In practice, "critical infrastructure" status is determined today on the basis of a number of criteria, including the number of people likely to be injured in a successful attack, the severity of the anticipated economic consequences and the impact on public morale.[§] Under these criteria, approximately 80 organizations

[§] Five hundred lives and a 0.5% loss in GDP were defined as the critical thresholds for inclusion in the list.

were initially identified as "critical," later reduced to about 30.[25] Inclusion on the critical infrastructure list does not necessarily encompass an entire organization. The electricity generation and transmission systems of Israel's national power company, for example, are defined as critical, whereas the billing system is not.[26]

The INCD National Cyber Security Strategy

Israel, as elaborated in Chapter 6, has yet to formulate an official national security strategy, or even a defense doctrine, and does not generate the type of fundamental strategic documents issued in the United States, UK, and other countries. In the cyber realm, Israel's early policymakers made a conscious decision *not* to adopt a doctrinal approach, in the belief that technology was evolving so rapidly that governmental policy would be unable to adapt quickly enough. Instead, they opted to establish a national cyber ecosystem, for which the government would provide overall guidance and regulation but in which it would not intervene directly. By 2017, however, the situation had crystallized sufficiently for the INCD to issue a National Cyber Security Strategy,[27] a broad statement of government policy in this area. The INCD Strategy focuses on the civil cyber realm, but also touches on issues of national security.[**]

In practice, the INCD Strategy was more of a conceptual elaboration of the principles and policies set forth in the cabinet decisions adopted between 2002 and 2015 than an entirely new strategic construct. Tellingly, some officials today are even unaware of its existence and believe that they are merely implementing the cabinet decisions.[28] Nevertheless, the strategy was presented to the premier and approved by him[29] and, as such, stands out as a significant departure from any previous Israeli decision-making praxis, the lone area in which Israel has formulated a comprehensive national strategy. Israel has yet to issue a similar public document in regard to terrorism, for example, an asymmetric threat that it has faced ever since its establishment.

The stated objective of the INCD Strategy is to:

> regulate all national efforts in the cyber security area, create a "common language" among those involved and provide a stable and long-term response in a manner designed to express the State of Israel's ongoing commitment to cyber security and to the preservation of the cyber realm as a secure space for economic and social prosperity.[30]

Beyond this, the strategy is essentially silent in regard to Israel's cyber objectives. It is, however, predicated on a number of fundamental assumptions.

[**] Figure 7.1 provides a timeline of all major governmental cyber decisions from the earliest days and through the implementation of the 2017 INCD Cyber Strategy.

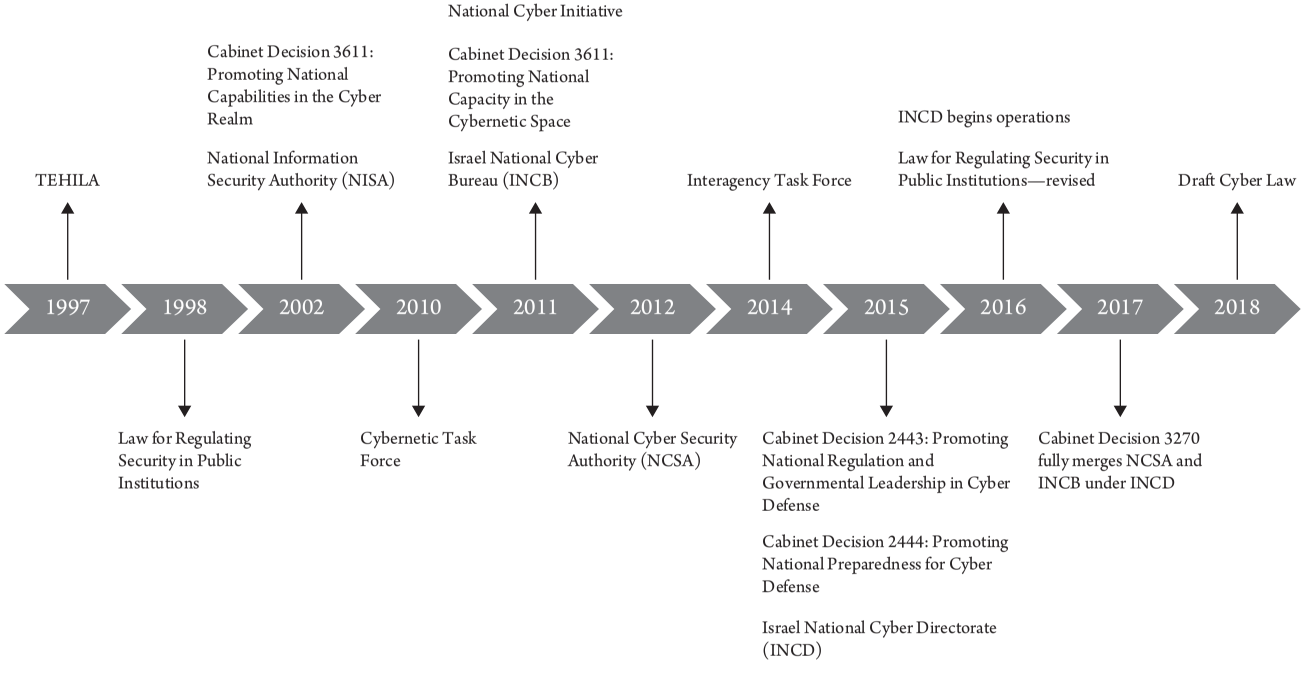


Figure 7.1 Cyber Decision Timeline

First, the cyber realm is largely a civil one, comprised of individuals and organizations, public and private, who are the targets of most of the attacks and in possession of most of the relevant information about them. Second, given the vast number of attacks, only these individuals and organizations can bear ultimate responsibility for their cyber security, but they generally lack the expertise and resources necessary to do so, thereby creating a role for the government.[31] Third, unlike the physical world, in which territory and populations are the primary targets of attacks, organizations and organizational processes are the primary targets in the cyber realm. Fourth, every computer system and network belongs either to an individual or organization and operates through an Internet provider, which is also an organization.[32] Fifth, the INCD focuses on the target of the attack and its ability to defend itself, whereas the IDF and intelligence agencies focus on deterring and thwarting the attacker.[33]

The INCD Strategy has four primary components: a concept of operations, defensive strategy, national cyber capacity building, and international cooperation, as follows.[34]

1. The Concept of Operations (CONOP)—addresses the entire range of cyber threats that Israel faces, but focuses primarily on the persistent and sophisticated ones, that is, those that pose a severe threat. The CONOP is based on three mutually dependent and complementary levels,[35] as follows, that constitute, in essence, a strategy of deterrence by denial.[36]

   Level 1: Aggregate Robustness—designed to strengthen the public and private sectors' overall ability to repel and contain cyber attacks, continue functioning even while under attack, and, in so doing, reduce the prospects of attack to begin with. Aggregate robustness is generic, that is, designed to provide effective responses to the entire range of potential attacks, and includes: organizational processes, such as risk management; technical measures, including system architecture, vulnerability identification, and authentication mechanisms; procedures focused on the human factor, such as personnel training and awareness programs; and cyber standards and regulation, best practices, preparedness plans, and more. Since organizations are the basic components of the cyber realm, they bear primary responsibility for robustness, with the state playing an incentivizing and supportive role.[37]

   Level 2: Systemic Resilience—designed to strengthen the state's ability to prevent and mitigate damage prior to, during, and following cyber attacks and to facilitate a rapid return to the antecedent level of functioning. Systemic resilience is necessary because robustness will fail at times, and some attacks will get through. Some of the capabilities needed for resilience are

in the hands of the private sector, including Internet providers, cyber security firms, and global corporations; some are state-based, such as systems to detect threats, share information and intelligence, assist in containing and recovering from attacks, and law enforcement; while others are in foreign hands. Unlike robustness, resilience is event-driven, not generic, and comes into play only when it has failed. Systemic resilience is also a cooperative undertaking and requires that organizations collaborate in order to fully leverage both their capabilities and those of the state, unlike robustness, which may be imposed by means of regulations and fines.

Level 3: National Defense—aggregate robustness and systemic resilience should be sufficient to prevent and contain most cyber attacks, up to 95% according to one estimate.[38] Much as in the physical realm, however, severe and persistent attacks may require that the entire range of state-based national security capabilities be brought to bear, including mechanisms for early warning and threat containment, defensive operations within the state's territory, and offensive measures outside of national boundaries, including the use of force. Whereas robustness and resilience focus on the targets of the attacks and the attacks themselves, efforts at this level are focused on the attacker and the state plays an exclusive role.[39] National Defense is essentially the only part of the INCD Strategy with clear military dimensions, which are further elaborated in classified annexes.

2. The Defensive Strategy—is based on centralization of authority in one operational agency, the INCD, which is responsible for both public and private sector cyber security and for promotion of a growing national cyber realm. In pursuit

Table 7.1 **The Concept of Operations**

Aggregate Robustness	*Systemic Resilience*	*National Defense*
Critical infrastructure regulation	Nationwide information sharing	Public and private sector defensive campaigns
Organizational and sectoral security guidance	Assistance to organizations under attack	Interagency coordination
National knowledge hub	Identification and investigation of attacks	National situational assessment
Cyber market regulation	Support for sectoral Security Operation Centers	—

Source: INCD, Israel's National Cyber Security Strategy, 2017.

of this role, the INCD leads national efforts to prevent, contain, and mitigate cyber threats to the public and private sectors, especially critical infrastructure and other vital systems; acts proactively to detect, locate, and investigate advanced attacks; manages or assists in the management of cyber incidents; serves as the interface between the public and private sectors and the defense establishment; and promotes the technological infrastructure necessary for secure organizational and individual cyber defenses. The defensive strategy includes:

Professional Guidance and Assistance in Organizational Defense—based on specially tailored defensive packages for critical infrastructure systems; regulation of those public and private sector organizations whose functional continuity affects the overall security of the national cyber realm (for example the financial, energy, and health sectors); and programs for promoting general public cyber security awareness and robustness.

Cyber Market Regulation—including licensing requirements for cyber professionals, products, services, providers, and networks. Israel's regulatory regime is based on the principles of proportionality, dynamism, use of international standards, and a degree of governmental involvement commensurate with the magnitude of the danger. In addition to the INCD, a variety of governmental authorities are responsible for sectoral cyber regulation. These authorities often lack sufficient cyber expertise, however, and thus work closely with the INCD for purposes of regulatory guidance.

Defense of the Governmental Cyber Realm—is critical to Israel's overall cyber security because of its magnitude, the sensitivity of the information contained and the potential impact on the economy and national life. Measures in this area include establishment of the GUCD and appointment of cyber directors in all government agencies; centralized regulation of governmental cyber procurement policies, risk management methodologies, and personnel hiring procedures; criteria for ensuring minimal cyber budgets in all governmental agencies; and technological measures to increase governmental cyber robustness.

Building Advanced National Cyber Infrastructure and Processes—to address gaps in the market's ability to provide appropriate solutions. Programs in this regard are designed, inter alia, to promote the cyber security and functional continuity of Israel's communications infrastructure in conjunction with ISPs; build the necessary infrastructure to facilitate adoption of secure and reliable identification processes; and develop the technological infrastructure necessary for government agencies, the defense establishment, and critical infrastructure.

3. National Cyber Capacity Building—through a centralized cyber ecosystem designed to promote entrepreneurship, technological innovation, and industry. National cyber capacity building includes, among other factors, cyber education programs starting in elementary schools, cyber research centers and education in the universities, R&D grants, and a variety of programs for developing cyber human resources and encouraging cooperation between Israeli and foreign firms.
4. International Cooperation—in recognition of the global nature of both cyber threats and opportunities, Israel cooperates with friendly countries in a variety of ways to help strengthen their common cyber security and participates in the international cyber discourse.

Defending the Civil Cyber Realm

In 2020 the INCD had an overall budget of approximately 250 million shekels (roughly $71 million) and a staff of some 350, including its operations center CERT-IL.[40] The INCD's ability to offer salaries far higher than is customary in the civil service, within 10–20% of the private cyber sector, along with the appeal of working on particularly challenging national issues have proven key to its ability to hire the appropriate cyber personnel in a highly competitive market.[41]

To help implement the National Cyber Security Strategy, the INCD published an Organizational Cyber Security Methodology in 2017.[42] This is designed to provide those public and private sector organizations that are *not* included on the Critical Infrastructure List, and thus do not enjoy specially tailored defensive packages, with detailed guidelines for identifying cyber threats and improving their security by themselves. It begins with a self-administered assessment of the dangers faced by the specific organization. Category A organizations, those that perceive little danger of cyber attack, can make do with a simple threat analysis and take only limited security measures. Category B organizations, those that perceive a significant threat and require stronger security measures, go through a more comprehensive process with detailed questions regarding the organization itself, the nature of the threats it faces, and its level of preparedness. The methodology then applies the Critical Security Controls approach developed by the SANS Institute, a world leader in the field, to recommend a comprehensive plan to promote the organization's cyber robustness and resilience, ensure its functional continuity, and specify the level of security appropriate to it.[43]

In 2018 the INCD issued the National Cyber Concept for Crisis Preparedness and Management, in essence a national cyber incident response plan with guidance on building crisis response teams.[44] The preparedness concept is based on

the assumption that effective preparation for crises is likely to reduce the risk of incidents actually evolving into full-blown crises, improve the management of those that do, and in so doing help ensure the functional continuity of core organizational processes. To this end, the preparedness concept recommends that both public and private sector organizations determine the vital cyber systems most relevant to them. The Organizational Cyber Security Methodology can provide an effective means of doing so and of determining whether a cyber attack is liable to cause substantial damage at the national level.

The preparedness concept further presents a multi-tiered cyber alert scale, ranging from the steady state, in which no there are no indications of a threat to the functional continuity of vital cyber systems, up to extensive and prolonged damage. Alert levels are determined on the basis of indicators in both the cyber and physical realms (e.g., military hostilities or natural disasters) and situational assessments. Finally, the preparedness concept provides a toolbox for mitigating cyber crises, based on measures designed to strengthen employees' professional expertise, including training and exercises, advance planning of how they will be deployed during crises, technological capabilities, and possible assistance from outside sources.[45]

Active Defenses—CERT-IL is manned 24x7 in order to respond to civil cyber incidents as they occur. Its responsibilities include developing proactive and reactive measures to strengthen the resilience of public and private sector organizations and assist them in coping with cyber threats and incidents; collecting actionable information (attack indicators, vulnerabilities, threats, malware) and procedures for sharing this information with public and private sector organizations; and serving as the interface between public and private sector organizations and the defense establishment.[46] As part of its intelligence collection responsibilities and as a means of anticipating and preventing future attacks, CERT-IL scours the Darknet and other odd parts of the Internet in search of relevant information.[47]

CERT-IL has two primary organizational sub-components: one processes calls from the public to determine whether an attack is an isolated incident or widespread, recommends initial means of addressing it, and, as appropriate, refers callers to the second component, the SOC, which can dispatch an Incident Response Team directly to an organization under attack and provide assistance in containing and minimizing the damage.[48] In conjunction with the relevant regulatory agencies, the SOC also operates special Sectoral Security Centers in a number of critical areas.[††] The financial sector CERT, for example, which

[††] The full list includes 15 critical areas, but, to date, not all of them are covered by sectoral SOCs: finance; communications; transportation; energy, electricity, and water; environmental protection; commerce and industry; local authorities; national government; domestic security; education; welfare; agriculture; science and technology, culture and sports; and religious services.

is operated jointly with the Ministry of Finance, Israel Securities Authority, and other regulatory agencies, has directed banks to formulate cyber security strategies, allocate the necessary resources, establish cyber security units headed by a senior official, monitor and supervise implementation of their cyber strategies, and report attempted attacks.[49] As of mid-2018, the SOC was in ongoing contact with 60 similar centers around the world and roughly 80 major organizations, most of them financial.[50]

In 2018 the then head of the INCD, Yigal Unna, announced that Israel would soon establish a framework for a "state-level defensive shield," designed to improve the overall level of national preparedness against cyber threats. This was to be achieved through improved detection, investigation, and mitigation of threats and further expansion of the already existing information sharing network between academic, commercial, and governmental institutions. The new shield was a further elaboration of the Digital Iron Dome concept announced the year before by Unna's predecessor, Eviatar Matania, and mentioned as early as 2012 by Prime Minister Netanyahu. According to Matania "the defensive shield . . . will not be one system, but a combination of several systems that will enable us to be in a much better place . . . you need something at the state level and this state level becomes the digital equivalent of the Iron Dome."[51]

Israel's active defenses include identification of Internet Service Providers (ISPs) most likely to be used to host an attack and providing cyber defenders with wide latitude to block traffic from them, for example, by allowing them to intervene even before an attack has actually begun or when it has been determined that the specific ISP is the conduit of the attack.[52] In 2019 the INCD introduced a new system for detecting attempts to deface websites called Trackzilla. The system has proven extremely successful, reducing, for example, the number of attacks conducted by Anonymous and other international hacktivists on Holocaust Remembrance Day from 1,145 in 2018 to just 134 the following year (see the #OpIsrael campaign in Chapter 4).[53] In 2020 the INCD deployed new capabilities in a variety of high priority areas, including secure AI, preparation for 5G, digital medicine, civil aviation, maritime cybersecurity[54] (possibly together with some of Israel's Mediterranean neighbors), protection of GPS systems, and more.[55]

Still another indication of Israel's active defenses can be found in an unusual tender issued in 2019 by the National Insurance Institute.[‡‡] The institute, which faces numerous cyber threats from within Israel and without, sought proposals for an active monitoring capability for social media, the Dark Web, Deep Web, and Clear Web.[56] This was also to include avatars, or fake profiles, and

[‡‡] Israel's equivalent of the US Social Security Administration.

be designed to defend not just against current attacks but to identify possible attacks in the future, for example, by monitoring a discussion among hackers regarding a vulnerability that they might have found in the institute's website. Complex and costly systems such as these are typically employed only by police forces and militaries.[57]

In 2017 growing concern over potential disruption of Israel's elections, following earlier attacks on the US and other electoral systems, led to heightened INCD involvement in the issue. Together with the Central Elections Committee, the INCD mapped out the threats and by 2018 a defensive strategy had been adopted. The test came in the four elections held between 2019 and 2021, in which the INCD set up a situation room in the Knesset, directly linked to the CERT-IL in Beersheba, with tens of cyber defenders at the ready. Every small computer glitch, of which there were more than a few, immediately aroused fears of cyber attack, but in the end the elections were conducted without mishap.[58] The INCD also cooperated with Facebook to remove thousands of fake profiles and bot accounts that had been created to spread false information about political candidates. A Facebook transparency tool, which bars anonymous political ads and ensures that users can identify their source, was also adopted, Israel being then only the fifth country to use this tool.[59]

In 2019 a special interagency team, headed by the INCD, together with the defense agencies, Ministry of Justice, and Central Elections Committee, found that Israel's low-tech, manual, voting system protected it from cyber attack, but that other parts of the electoral process, including the computer systems, websites, and smartphones belonging to the political parties and Central Elections Committee, were vulnerable.[60] It thus recommended that the manual voting system be retained and new procedures be implemented to further secure the other parts of the electoral process.[61] In 2022 the State Comptroller, a respected watchdog agency, recommended that the issue of computerized voting be reviewed, but echoed the need for strengthening the cyber security of other parts of the electoral process. To this end, it further recommended that the INCD provide the Central Elections Committee with professional guidance on an ongoing basis, not just during elections, and that its guidance be binding.[62]

Ongoing concern over the potential impact of information operations against Israel led in 2021 to the establishment of an interagency committee chaired by the director general of the Ministry of Justice. The committee was given a broad mandate to make recommendations regarding Israel's policy toward social media and the major tech firms, including such matters as privacy rights, slander, taxation, intellectual property, and criminal law.[63]

In 2020 the government issued an RFP to build a cloud infrastructure facility in Israel, designed to house all governmental and IDF systems, to replace the European-based facility currently in use. Cloud facilities such as these typically

serve a number of countries, meaning that one built for Israel alone would be of questionable economic viability. For security reasons the government was interested, nevertheless. The new facility is to have two locations: a highly secure one for governmental and defense agencies and another for the commercial sector. As an inducement for the multinational tech corporations to build the cloud infrastructure facility, the government undertook to encourage as many Israeli firms as possible to use it and to award the company that built the facility both the government's entire annual IT budget, worth approximately $150 million, and the IDF's. The estimated construction cost of a facility of this sort, usually built underground, is about $500 million.[64]

Nongovernmental "patriotic hackers" present an entirely different form of active defense. Nongovernmental Israeli hacking groups defaced websites used to conduct waves of cyber attacks against Israel during the conflict in Gaza in 2014 and have taken others off-line.[65] In 2015, in response to the leak of 150,000 Israeli phone numbers and email accounts by Anonymous, a group of nongovernmental Israeli hackers leaked the Palestinian Population Registry, with data on four million Palestinians, as well as the personal information of some 700 Palestinian journalists and employees of the Palestinian Authority. In 2016, in response to that year's #OpIsrael campaign and attacks on the websites of Yad Vashem[§§] and other governmental institutions, a different nongovernmental group, the Israeli Elite Force, exposed the names, pictures and addresses of the US, British, German, French, Turkish, and Lebanese hackers involved.[66]

A final form of active cyber defense is the use of fish—not phish, fish. Following a cyber attack on the national water system in 2020, Israel's water company deployed a variety of cyber defense mechanisms to monitor changes in water quality, along with fish in an aquarium, much like the proverbial canary in the coal mine.[67]

Information Sharing—CyberNet facilitates information sharing about attacks between CERT-IL, the government, and public and private cyber security teams and in 2020 had 1,500 users. Much of the information is sensitive from an intelligence perspective, but the sources are disguised in order to enable its distribution.[68] In 2019 CERT-IL established the world's first cyber hotline to report attacks to individuals and organizations and provide them with real-time assistance.[69] In 2020 14,300 incidents were reported, of which 9,100 were confirmed as actual cyber incidents. Of these, 60% were social media attacks, and over 20% were attempted penetrations into data and communications networks.[70] In one major case in 2020, more than 3,000 organizations were contacted and issued specific instructions regarding means of preventing the attack and mitigating the

[§§] Israel's national Holocaust memorial.

damage. CERT-IL also handles numerous reports each day from international partners.[71]

Cyber Exercises—Much as in the physical world, cyber training exercises are essential in order to maintain effective cyber defense. The IDF, INCD, and other agencies conduct simulations of cyber attacks against Israel by state and non-state actors to determine where its defenses are weakest and improvements are necessary.[72] Israel conducted its first national cyber emergency exercise in 2012. Dubbed Lights Out, the days-long exercise tested Israel's readiness in the face of a cyber attack designed to paralyze its critical infrastructure and cause severe disruptions to public life.[73] The annual home front exercise in 2015, Turning Point 15, simulated cyber attacks that succeeded in bringing down the electric grid and phone system. The national home front exercise in 2021 simulated power outages due to cyber attacks that lasted for three days.[74]

In 2018 Israel held Vicious Cycle 2, the most complex cyber exercise it had conducted up to that time and the largest in terms of the number of agencies involved. The simulated scenario included cyber attacks on governmental, public, and private sector institutions and was designed to test Israel's readiness at the national level, including cooperation between the different agencies, operational plans for thwarting attacks, dissemination of information, legal issues, and more.[75] In 2019 the INCD, Bank of Israel, Ministry of Finance, Israel Securities Authority, and a variety of other government institutions conducted a first of its kind exercise to test the financial sector's ability to continue functioning under cyber attack at the same time that a military confrontation was underway in Gaza. Among other issues, the exercise simulated the institutions' ability to continue to make governmental transfer payments, pay claims, manage investments, and conduct customer relations. One of the conclusions was that financial institutions either lacked procedures for resiliency or those in place were insufficient.[76]

The Cyber Law—in 2018 the INCD circulated a draft proposed new Cyber Law for comment by other governmental agencies and the public at large. The draft law reflected four key assumptions that have long guided cyber policy in Israel, including the establishment of the INCD: that public and private sector organizations are the primary targets of cyber attacks and in possession of most of the information needed to address them, consequently only they can bear ultimate responsibility for their defense; that these organizations typically lack the requisite expertise and resources to defend themselves against the entire range of threats they face, thereby necessitating governmental assistance; that an effective response to the cyber threat requires a coordinated national approach; and finally that the existing division of authority between the defense agencies in the cyber realm was not to be adversely affected by the INCD's establishment.[77]

The draft law had three main parts: an organizational chapter, which outlined the INCD's areas of responsibility; a public and private sector cyber security chapter, which addressed some of the means of detecting threats and of defending against them; and a regulatory chapter. The organizational chapter defined the INCD as an operational defense agency responsible for protecting the public and private cyber realms against threats to "vital national interests" and for promoting Israel's standing as a global leader in the field. The INCD was to deal with the targets and results of attacks, while the defense agencies would continue to bear responsibility for countering both the attacks and attackers themselves. As with the various cabinet decisions adopted over the years, the draft law did not fully resolve the outstanding issues regarding the division of authority between the INCD and defense agencies.

The draft law emphasized the importance of the regulatory system's national security dimensions, which cannot be measured solely in monetary terms and must be flexible in order to adapt to rapidly changing circumstances. It thus directed the INCD to develop a "methodology" for determining whether a "vital interest" was at stake. The methodology was to be based on a number of factors, such as: the level of service required of the organization both under routine operations and during times of emergency; the size of the population affected; the potential for loss of life, economic damage, environmental harm, and damage to privacy; the extent and sensitivity of the information affected; and the impact on computer and Internet services, resources, services, manufacturing, and other processes of critical importance for the public, economy, and defense agencies.

In order to prevent cyber attacks that pose a threat to vital national interests—and subject to the consent of the specific organization or individual under attack—the draft authorized the INCD to enter any governmental, commercial, public, or residential space, issue instructions on remedial measures to be adopted, and take possession of any item believed to contain relevant information for a period of up to 90 days. It also authorized the INCD to do this *without* the consent of the organization or individual, but with a court order and if one of three conditions applied: the attack posed a danger to Israel's entire cyber ecosystem, the organization under attack was of national importance, or the attack was conducted by a hostile foreign actor.[78]

The draft law stated explicitly that interventions were to be conducted solely for reasons of national security, to identify the extent of an attack, prevent or at least contain the damage, and remove the threat, not for purposes of law enforcement or to monitor the activities of the individual or organization involved. The information gathered was thus to be limited to meta data and machine language, not the substance of the communications. Interventions were also to be subject to the principle of proportionality, that is, that the harm to privacy and organizational functionality would be the minimum necessary given the magnitude of

the threat and less than the benefits derived. Moreover, an intervention would only take place if an individual or organization was unable to take appropriate measures on their own. To encourage individuals and organizations to cooperate with the INCD voluntarily and reassure them regarding the intervention's transparent nature, the draft law guarantees their right to know the nature of the information collected, subject only to certain operational considerations.[79]

Under the draft law, Israel was to have a hybrid regulatory system—centralized, decentralized, and mixed—designed to strengthen public and private sector robustness and resilience, but also to reduce the regulatory burden to the minimum necessary and ensure the private sector's ability to innovate in response to rapidly changing market demands. The regulatory system was to be based on accepted international standards while taking into account the type of organization, nature of the threats it faced, likelihood of their actually materializing, direct costs of regulations to businesses, and effect on business activity as well as competition and consumer satisfaction. The proposed regulatory system was to empower existing regulatory agencies, rather than lead to the establishment of new ones. These agencies would be authorized to issue licenses and certifications, and corporate boards would be required to submit annual reports regarding the cyber threats they faced, the resources they had allocated for cyber security, and the name of the individual responsible for corporate cyber security. Some public and private firms, not on the critical infrastructure list, would also be required to mitigate the dangers of cyber attack and report data breaches to the government or customers.[80]

The proposed hybrid regulatory system was to be based on three types of organizations.

- **Category A**—organizations whose disruption posed a *severe* danger to Israel's vital interests, a few hundred in all. Those Category A organizations defined as critical national infrastructure would be subject to a decentralized regulatory model, under the INCD's supervision, others to a mixed, centralized and decentralized, model. Where sectoral regulatory agencies exist, the INCD's role would be limited to enhanced oversight; where they do not, it would exercise direct oversight, either temporarily or permanently. Specially tailored defensive programs would be provided to all organizations in this category.
- **Category B**—organizations whose disruption posed a *significant* danger to Israel's vital interests, a few thousand in all. These organizations would be subject to a decentralized regulatory system, based on the existing regulatory agencies and the INCD's professional guidance.
- **Category C**—organizations whose disruption posed *little* danger to Israel's vital interests, in effect, all those not included in Categories A or B (i.e., the

rest of the economy). Only "soft" and voluntary measures would be applied to these organizations, such as training and awareness programs.

In recognition of the sensitive civil liberties involved, the draft law provided for the establishment of two special oversight functions to ensure compliance with privacy rights. One, an "internal privacy supervisor," was to be an INCD official responsible for helping to shape decisions prior to their adoption and undertake post-facto review of measures already taken. The second was to be an independent Supervisory Committee, chaired by a senior legal figure and comprised of representatives of the Attorney General, INCD, and public at large. The draft further specified the conditions in which measures taken to ensure the security of an individual's or organization's computer systems, or to share information with other organizations, would not be deemed violations of antitrust and privacy laws, or laws against wiretapping and illegal computer intrusions.[81]

Israel's civil liberties organizations pushed back strenuously against the draft law and a variety of important changes were made (which have been incorporated into the outline presented here).[82] More surprising, perhaps, was the virulent opposition from the defense establishment. In a highly unusual and possibly unprecedented move, the heads of the four primary defense bodies—the IDF, ISA, Mossad, and Ministry of Defense—submitted a joint letter to the prime minister and cabinet asking that the proposed legislation be amended. The defense chiefs charged that it greatly expanded the INCD's authority, undermined their organizations' ability to deal with the cyber threat and warned of severe harm to Israel's defense interests.[83]

In early 2021, in what may have been an attempt to take advantage of the electoral chaos at the time, the government sought to pass an abridged version of the proposed law focusing primarily on public and private sector cyber security, without the detailed sections on national cyber organization and regulation. The abridged proposal was to be a provisional law, in force for just two years, to facilitate passage by the Knesset, but its backers presumably hoped that it would become permanent once enacted. Once again, public controversy focused primarily on the dangers to rights of privacy stemming from the authority that would have been given to the INCD to enter any premises for cyber security purposes.[84]

Further contributing to critics' concern, the abridged bill significantly expanded the ISA's role in both public and private sector cyber security. In the event of severe cyber attacks, the ISA was to be authorized to take the same measures as the INCD, that is, to enter any premises, assume possession of equipment and data, and issue remedial orders, subject only to specific approval by the head of ISA and post-facto reports to the prime minister and head of the INCD. Relatedly, INCD officials would be authorized to request that the ISA—and

ISPs—provide them with information regarding the identity and contact information of various individuals and organizations within 72 hours, provided only that they were at risk of or actually under cyber attack.

The abridged cyber bill further expanded the definition of the "vital interests" necessary to justify INCD intervention in organizational or private premises. Instead of the more specific and even quantitative standards set out by the previous draft, including specified levels of damage to the economy, loss of life, and harm to national security, the definition now took on a more ambiguous nature, such as "prevention of severe damage to public welfare" and "protection of the environment." The definition of "vital" organizations was also expanded, so that all organizations that conduct activities of concern "to the entire public or significant parts thereof," as well as communications and Internet providers, would come under the purview of the INCD and ISA.[85]

Some critics charge that the abridged bill constitutes a paradigm shift, changing the INCD from a policy and regulatory body that works with the public and private sector organizations on a voluntary basis into an operational agency with enforcement powers. Rather than relying on these organizations' voluntary but vested institutional interests in protecting their data, clients, and systems, the abridged bill would shift responsibility for cyber security to the government (the INCD) and make compliance compulsory. Whether public and private sector organizations have, in fact, cooperated sufficiently with the INCD, or not, thereby necessitating the additional powers granted, is the subject of debate.[86]

At the time of this writing, it remains to be seen what form the final bill will take, if any, but domestic and bureaucratic politics have already had an important impact on it. Substantive differences, as well as the decision-making stasis stemming from Israel's political crisis of 2019–2021 and the Covid-19 crisis in 2020–2021, have left it in limbo.

The INCD at Five; A Midterm Assessment

Some five years after the INCD's establishment, it is hardly surprising that it has yet to fulfill all of its goals or that it is the subject of criticism from both within government ranks and without. Some of the criticism is focused on the overall strategy, as embodied both in the cabinet decisions adopted between 2002 and 2015 and the formal 2017 INCD Strategy, some on their implementation in practice.

In 2016 the State Comptroller issued a report that was highly critical of Israel's preparations for the cyber threat. The report charged that the lengthy period required to adopt the cabinet decisions, establish the necessary agencies,

and enact legislation had caused a delay in the government's original timetable for addressing both the cyber realm's threats and opportunities and that a considerable gap thus existed between the magnitude of the challenge and Israel's response.[87] This criticism was echoed later that year by the Knesset Subcommittee on Cyber Defense, which also found Israel's preparations to be deficient.[88] Follow-up reports by the State Comptroller in 2019 and 2022 found that procedures established for protecting critical infrastructure, including the particularly important Israel Electric Corporation, as well as sectoral defenses, had only been partially implemented.[89]

Critics of the 2017 INCD Strategy note that it essentially did not set out the objectives to be achieved, normally the bedrock of any strategic document, and instead turned directly to the proffered solutions.[90] This lacuna is further compounded by the nature of cabinet decisions in Israel (*hatzaot machlitim*), which are operational documents outlining the measures to be taken, without a detailed statement of the strategy and policy objectives to be achieved. There is little doubt that the cabinet decisions adopted between 2002 and 2015 reflected a broad and well thought out strategy, but the nature of the decisions is such that we are not a party to the thinking behind them. The 2017 strategy document was a missed opportunity to rectify this.

In the absence of carefully defined objectives, the 2017 strategy also did not present a multiyear work plan, which would have provided a clear path forward for the INCD and other actors in Israel's cyber realm.[91] The absence of a plan of this sort is not unusual, few agencies in Israel formulate one and the extraordinarily rapid rate of change in the cyber realm makes it particularly difficult. Yet the INCD was a forward-looking agency from the outset, the first to draft a comprehensive national strategy, and would have benefited from such a multiyear plan. The IDF, arguably the governmental body with the most sophisticated planning capabilities in Israel, considers its five-year work plans critical to its ability to function and has assiduously formulated them for decades, even if changing constraints have meant that implementing them in practice has proven difficult.

Another criticism is that the strategy, as embodied in the cabinet decisions and 2017 document, is already partially outdated.[92] This is hardly a stinging rebuke considering the frenetic pace of change in the cyber realm and the fact that the INCD Strategy was more of a conceptual explication of the decisions the cabinet had adopted in 2015 than an entirely new strategic statement in its own right. Be that as it may, Israel was among the first states to develop a comprehensive response to the threats and challenges posed by the cyber realm and is worthy of appropriate approbation.

A further criticism is that the INCD Strategy was overly focused on public and private sector cyber security and that a more holistic approach was necessary. Other than a few generalities, it is silent regarding Israel's approach toward

defense in the military cyber realm and makes no reference to cyber offense. This is not entirely surprising in a public strategy, and both the cabinet decisions and the INCD Strategy[93] had classified annexes that at least touch on the military dimensions, although we are in the dark beyond this. Nevertheless, critics contend that at least some reference might have been made to a variety of fundamental and arguably less sensitive issues, such as the types of targets that Israel believes can legitimately be attacked by cyber means, the circumstances and means (whether cyber or kinetic) with which Israel might respond to cyber attacks, and its thinking in regard to the creation of cyber deterrence.[94] Whether one agrees with these specific points, or not, other states have set out unclassified military cyber strategies without harm to their national security, and Israel could certainly have said more than it has.

More to the holistic point, some critics argue that the INCD Strategy is overly operational and too focused on the INCD itself. As a result, it does not recommend ways of promoting the cyber ecosystem, explain how Israel is to utilize its cyber capabilities to achieve broader national objectives, or identify important areas for future change and improvement. The role of other government agencies, such as the Israel Innovation Authority, is also not mentioned, nor are Israel's policies regarding emerging technologies.[95] The 2017 Strategy and cabinet decisions, indeed, provide only scant details regarding promotion of the cyber ecosystem, and there is certainly a need to set out a longer-term vision. As will be seen in the following chapter, the cyber ecosystem is an area in which Israel has excelled, and yet there are clouds on the horizon that make this criticism an important one.

The 2017 Strategy and cabinet decisions are also faulted for no more than a cursory mention of the importance of international cooperation as a means of promoting cyber security and of Israeli participation in international cyber discourse. Israel's positions regarding international cyber norms and law, or export controls, are not mentioned, nor are the considerable benefits that states stand to gain from cooperating in this area. The benefits that Israel itself can derive from international cyber cooperation, such as state-of-the-art technology that it currently lacks in key industries, are also not mentioned.[96]

For all of its shortcomings, the bottom line is that Israel developed and implemented a coherent and well thought out national cyber strategy and the INCD has assumed a place of importance in Israel's national security and economic realms and has done an impressive, if imperfect, job in fulfilling its tasks in challenging circumstances. Israel, today, is considerably better defended than in the past and, as we saw in Chapters 4 and 5, remarkably few successful cyber attacks of significance have taken place. Partly, this may be because Israel has not wished information to get out, but it is mostly because of the quality of its strategic thinking and defenses, which draw on the comparatively high degree of

cooperation manifested by the different sectors of Israeli society, the IDF, government, industry, private sector, and academic institutions. As a result of Israel's circumstances, size, and culture, these sectors have manifested a willingness to work together under strong centralized authority to a degree that would be hard to find in many other democracies.[97] Chapter 8 addresses these and other dimensions of Israel's national cyber ecosystem and capacity building.

8

National Capacity Building

The biggest secret of the Israeli high tech system is the military's ability to look at people while they are in high school.

Nadav Zafrir, former Commander of Unit 8200, now high tech entrepreneur

Technological prowess played a critical role in Israel's national security doctrine and economic policy from the earliest days. The cyber realm, with its emphasis on outstanding scientific and technological creativity and innovation and potential for rapid and high returns on investments of a comparatively modest scale, was considered to be particularly suited to Israel's national strengths. It was also particularly suited to Israel's strategic culture and national temperament, or what we call chutzpah gone viral. Over the years, these basic national cultural characteristics fused with the strategic and economic imperatives to improvise and innovate. In the process, they became deeply ingrained, almost reflexive Israeli traits, a national modus operandi and sphere of excellence, often manifested even when more established and routinized modes of operation might be preferable. The IDF and intelligence agencies, which have an unusually symbiotic relationship with the civil cyber sector,[1] are also deeply imbued with this innovative national culture and have become primary engines thereof, further promoting cyber and Israeli high tech in general.

It is here that the constructivist concept of strategic culture meets the realist concept of creative insecurity. Strategic culture, as already noted, refers to the impact of a state's historical beliefs, collective memories, values, traditions, mentality, and strategic assumptions on its national security decision-making.[2] Creative insecurity arises when significant external threats, economic and/or military, incentivize scientific and technological innovation designed to foster and sustain an internationally competitive economy, thereby enabling the state to purchase the means to defend itself or build domestic defense industries.[3]

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0009

Both concepts are highly applicable to Israel, which recognized from the beginning that the cyber realm's unique blend of civil, commercial, criminal, counterterrorism, and military dimensions required governmental leadership and a "whole of society"[4] response. To this end, a variety of policies and programs have been developed to foster Israel's overall cyber capabilities—in sum, a national cyber ecosystem. Developing this ecosystem has been a basic aim of Israel's cyber policy and of every cabinet decision in this regard ever since the first one was adopted in 2002.[5]

Chapter 8 has three sections. The first presents an overview of Israel's civil cyber ecosystem, tracing such issues as investment in cyber R&D, comparative indices of Israeli innovation, the size of Israel's high tech and cyber sectors, numbers of cyber firms, and more. The second section addresses some of the reasons for Israel's success in the high tech and cyber areas and is divided into four subsections: cyber R&D and technology spillovers, development of cyber human resources, Israel's innovative cyber culture, and social networks. The chapter concludes with a discussion of some of the clouds on Israel's high tech and cyber horizons, possible misdeeds in the cyber realm, and new opportunities for technological development.

Building Cyber Industry: From Jaffa Oranges to Silicon Wadi

The reason why Israel has come to be known as the startup nation clearly emerges from the numbers. Israel's economy is the most tech-dependent in the world, with 13% of GDP and 31% of exports originating from the high tech sector. Israel has long been ranked first in the world in terms of investment in R&D and venture capital, as a percentage of GDP, approximately double the OECD average. If one adds military R&D, the gap is even larger, with an additional 1–1.5% of GDP.[6]

Israel has the largest number of high tech startups per capita in the world,[7] with approximately 600 new ones established on average each year, making a total of roughly 6,000 in 2019. Israel has the second largest number of firms listed on the NASDAQ of any country outside of North America.[8] In 2020 Israeli startups raised $11.5 billion, 20% more than 2019 and more than four times the amount raised a decade earlier.[9] In the past, Israeli high tech firms were considered to be excessively focused on short-term gains and a rush to go public, rather than taking a longer-term perspective designed to build a significant international presence. This is no longer the case. Israel already had more "unicorns" (firms with a worth over $1 billion) per capita in 2020 than any other country

in the world, indeed, almost double the rate in the United States; and with just 0.1% of the global population, it had one third of all cyber security unicorns. While only 10% of startups globally usually survive more than five years, in Israel the comparable figure is a whopping 65%.[10]

In 2020 the World Economic Forum ranked Israel the sixth most innovative nation in the world, down from second place in 2016–2017, but still very high. The study was based on 12 indices of competitiveness, including innovation, technological readiness, business sophistication, higher education, patent filing, R&D expenditure, and more. In 2021 a Bloomberg study, based on seven indices of innovation, placed Israel in seventh place, down two notches from where it had been two years earlier, but still ahead of its tenth-place ranking during the two years prior to that.[11]

Israel has one of the world's highest concentrations, per capita, of technologically advanced human resources. It has the highest concentration of scientists of any country, 135 for every 10,000 people, compared to 85 in the US; ranks first in the world per capita in research personnel and third in university graduates; and is consistently ranked among the top ten in patent applications.[12]

There are nearly 400 multinational R&D centers in Israel, including more than 25 in the cyber realm alone. On average, 22 additional R&D centers open each year.[13] The list of multinational corporations that have set up R&D centers in Israel reads like a Who's Who of the top firms in the field.* These firms employ tens of thousands of people and are involved in the development of highly advanced systems. Microsoft's Israeli R&D center, for example, is one of three "strategic global development centers" and is considered home to some of the company's most innovative technologies, with a focus today on big data, business intelligence, cloud storage, and artificial intelligence. Many of these multinational companies have also bought numerous Israeli startups.

In recent years Israel has become a growing center of startups in the "smart transportation" sector. Global giants, such as General Motors, Ford, Renault-Nissan-Mitsubishi, Hyundai, and Volkswagen, among others, have established research centers in Israel dealing with autonomous mobility, vehicle technology, and more.[14] Israel is also poised to become a significant player in what has been dubbed the Fourth Industrial Revolution, also known as Industry 4.0, the Industrial Internet of Things (IIoT), and smart manufacturing. As of 2019, 230 companies were active in Industry 4.0 in Israel, an increase of 60% over 2014, including 23 R&D centers, 11 hubs, and 8 accelerators and incubators. Venture capitalists have taken note of the potential, and venture capital financing for

* Intel, Google, Microsoft, IBM, Amazon, Facebook, Deutsche Telekom, HP, Cisco, Marvell, Apple, McAfee, EMC, PayPal, Oracle, General Electric, and Lockheed Martin, among others.

these firms in 2018 accounted for 5% of all global financing in the field. The government has also earmarked over $100 million to support the transition of the local manufacturing industry to IIoT.[15]

Israel's high tech sector employs approximately 300,000 people, or 9% of the total national labor force, including 50,000 software engineers. The cyber industry employs 20,000 people (not including defense firms), of whom 7,000–8,000 are engineers.[16] The high tech sector is based around four primary hubs—Tel Aviv, Haifa, Jerusalem, and Beersheba—and a number of smaller satellite ones, but really all constitute one region. The greater Tel Aviv hub, the heart of the Israeli high tech ecosystem, is widely considered the second most important in the world, after Silicon Valley. Much of the activity is centered on Tel Aviv and Bar Ilan Universities, the Weitzman Institute, and the many advanced IDF bases in the area. More surprisingly, Jerusalem, with its large traditional and ultra-Orthodox populations, has become a flourishing center for biomed, cleantech, Internet/mobile startups, accelerators, and the support of service providers. The total number of high tech firms in Jerusalem doubled between 2012 and 2020, many of them centered around Hebrew University.[17] Haifa, which blazed the way in the early years of Israel's high tech revolution, has lost its leading role, although the Technion remains Israel's premier institute of higher education in technological fields.

As early as 2015 Israel had over 300 startups focused on the cyber realm, double the number five years earlier and, remarkably, equal to the total number of such firms in the rest of the world combined, not including the United States. By 2019 the number of cyber startups had grown to 436, out of all 752 cyber firms in Israel, making it the world's second largest exporter of cyber security software.[18]

Between 2013 and 2017 Israeli firms accounted for 7% of all global cyber security trade, ahead of Britain, Canada, and China.[19] In 2016 Israeli cyber exports reached $6.5 billion, equal to 8–10% of a global market estimated to be worth roughly $70 billion;[20] in 2021 they were worth $11 billion.[21] In terms of foreign direct investment (FDI) in cyber security firms, Israel is again second only to the United States. Between 2013 and 2016, FDI in Israeli cyber security firms grew from $165 million, about 11% of the world total, to $500 million, or 15% of the world total at the time.[22] In 2020, 31% of cyber investment worldwide was in Israel, an increase of more than 70% over the previous year and a 50-fold increase over the previous decade. Altogether, over 20 cyber firms were purchased with a combined value of some $4.7 billion. Israel never previously enjoyed such dominance in any technological area.[23]

The hub in Beersheba starts at a disadvantage, given its distance from the center of the country and less attractive desert environment, but the government has officially declared its intention to turn the city into Israel's "cyber

capital." Beersheba's Advanced Technology Park (ATP), called Cyber Spark, was established in 2013 as a joint venture of the government, local municipality, and Ben-Gurion University (BGU) and is at the heart of these plans. It is also an important example of the national policy of promoting heightened cooperation in the cyber realm between academia, multinational corporations, startups, government agencies, and the IDF, all of which work in the ATP office complex and have the opportunity to assist each other with knowledge, personnel, and resources and to foster new innovative ideas. To encourage firms to open offices in the ATP, the government offers grants covering up to 20% of salaries. In 2019 some 70 firms had offices there, ranging from global giants such as Lockheed Martin, IBM, Deutsche TeleKom, and EMC to small startups. The ATP also houses the INCD's national cyber emergency response team (CERT-IL) and personnel from a number of IDF units and the ISA.[24]

The IDF is slated to play an important role in Beersheba's cyber ecosystem. Its new national cyber center, adjacent to the ATP, is scheduled to be completed by 2023. The center will house the C4I and Cyber Defense Branch's[†] technological units and computer, cyber and communications schools, as well as some Air Force and other units. The thousands of soldiers serving at the center will be able to register for courses at BGU.[25] The IDF also plans to relocate intelligence units, including Unit 8200 (Israel's equivalent of the US National Security Agency), with a combined staff of approximately 19,000 people, to a new base near Beersheba.[26]

Israel's unique cyber ecosystem is based on unusually close collaboration between the government, defense establishment, academia, and commercial sectors.[27] In an area changing as rapidly as the cyber realm, in which a technological generation is no more than 1.5 years, it is impossible to predict all threats and opportunities. Israel's cyber ecosystem was thus designed to be highly flexible and capable of evolving in accordance with the frenetic pace of technological change.[28] To this end, while the government was deeply involved in promoting the cyber ecosystem in its early years, especially industry and academia, it has become essentially autonomous in the interim, capable of standing on its own. Indeed, the INCD has concluded that the cyber industry no longer needs significant governmental funding, given the large sums readily available from the private market, and it is now exploring new ways in which the government can best be of help.[29]

[†] C4I—command and control, computers and communications. The branch is responsible for IDF communications and computer systems and cyber defense.

Cyber R&D and Technology Spillovers

From the beginning, cyber R&D (academic, commercial, and military) has been one of the primary means by which Israel has sought to achieve and maintain a lead in the global cyber realm.[30] In the academic area, the INCD matched the universities for a total investment of some 250 million shekels in order to encourage the establishment of cyber centers at each one. Each university was free to decide where its strengths lay and which areas it wished to focus on.[‡31]

Ever since 2012, the INCD has provided hundreds of millions of shekels to Israel's universities for research. In 2013, there were approximately 30 academic cyber researchers in Israel; by 2019 the number had reached 200.[32] The INCD and Israel Innovation Authority (IIA)[§] fund programs designed to promote cyber R&D and entrepreneurship. Of 2,875 R&D funding requests submitted to the IIA in 2018, it invested in 920 firms and provided 1.7 billion shekels (nearly $500 million) in funding for approximately 1,500 projects.[33] The IIA further provides direct assistance to firms engaged in cyber R&D, as well as matching grants with third parties, both Israeli and foreign. Unlike INCD projects, which typically focus on governmental or military cyber capabilities, IIA assistance is designed solely for commercial projects and dozens have been funded with firms from states around the world.[**] The IIA and Ministry of Science and Technology also offer scholarships and research grants in the area of cyber security.[34]

Israel further seeks to promote cyber R&D through cooperation with leading multinational high tech firms. Deutsche Telekom, for example, which is already involved in the Cyber Spark ATP in Beersheba, has expanded its collaborative efforts with BGU, with a focus on network security and big data. IBM established a research center there focused on big data, cloud computing, cognitive cyber protection, security of connected vehicles, and biometric authentication. Fujitsu established a cyber security center at BGU focusing on developing security technologies for AI-based systems. Germany's Fraunhofer Institute for

[‡] The cyber center at BGU, Cyber@BGU, focuses on technology and applied science. Hebrew University's Cyber Security Research Center specializes in security and cryptography, as well as international law in the cyber field. The Technion's Hiroshi Fujiwara Cyber Security Research Center focuses on software and hardware protection, as do Haifa University's Center for Cyber Law and Policy and Bar-Ilan University's Research Center in Applied Cryptography and Cyber Security. Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center takes a broader interdisciplinary approach, including policy and legal issues.

[§] Formerly known as the Office of the Chief Scientist, IIA is under the Ministry of the Economy and Industry.

[**] Among others, the United States, Singapore, South Korea, Canada, China, Japan, India, Australia, and Latin America, in addition to a number of multilateral European projects.

Secure Information Technology established a joint cyber research center with the Hebrew University in Jerusalem.[35]

The IDF and Cyber R&D—the contribution of the IDF, intelligence agencies and the defense establishment, as a whole, to Israel's high tech capabilities, cannot be overstated. Much like the Department of Defense in the US, and especially the unique role played by DARPA (the Defense Advanced Research Projects Agency), the defense establishment in Israel and its DARPA equivalent, MAFAT (the Directorate of Defense R&D), have been among the driving forces behind innovation in Israel.[36]

In practice, the MoD, IDF, especially Military Intelligence Units 8200 and 81 (the advanced technologies unit), and various IAF and C4I Branch units have become important incubators and accelerators of high tech startups, with knowledge, capital, and resources flowing to the private sector—and vice versa. This is especially true in the cyber realm, where the defense establishment's deep involvement in defense related cyber R&D has spawned numerous civilian applications. Many of the leading high tech and cyber firms in Israel—Check Point, Palo Alto Networks, and NICE Systems to mention just a few—were founded by people who had served in Units 81 and 8200 and other leading IDF units.[37]

Intelligence Unit 81 is the most decorated unit in the IDF, having won an extraordinary 36 prestigious annual Israel Defense Prizes for technological innovation. A top-secret unit whose motto is "turning the impossible into the possible," Unit 81 is at the forefront of global technology. Approximately 100 veterans of the unit, who served between 2003 and 2010, founded 50 startups during the following decade alone, with accumulated valuations exceeding $10 billion. One unit veteran, who founded a number of highly successful startups, explains this unusual entrepreneurial success rate this way: "A team that has worked together before is a substantial force multiplier. You can't find that in Silicon Valley, either in terms of the pool you can draw from, or in terms of knowledge and experience. Even Google and Microsoft don't have a concentration of talent like Unit 81."[38]

The IDF, IAF, and MoD, in collaboration with a private firm, launched an innovation center in 2019—dubbed INNOFENSE—designed to promote the development of new technologies and innovative startups. The center focuses on civilian cyber technologies with military applications, such as big data, the IoT, unmanned systems, robotics, cyber, deep learning, homeland security, and border security.[39] The IDF also launched two other programs, Stargate and Star Trek, the first of ten planned programs that apply AI to interpret intelligence information for operational purposes. In the past, sensitive and sophisticated software of this sort would have been developed by the IDF solely in-house, but the need for personnel with unique expertise and the push for more rapid

development times has led to growing cooperation with commercial firms. The ability to use the sophisticated code developed—minus the sensitive defense applications—is the private firms' primary commercial incentive for participating in these programs.[40]

The Mossad, similarly, has established Libertad, a technology innovation fund that invests in startups in a variety of areas, including financial tech, robotics, AI, drones, remote personality analysis, natural language processing, voice analysis and processing, synthetic biology, Blockchain, and online privacy. Investments are made on particularly attractive terms for the entrepreneurs; in return, the Mossad gains access to unique intellectual property, without retaining commercial rights after the R&D stage is over.[41]

Cyber Human Resource Development

In the early 2010s the INCD,[††] IDF, Ministry of Education, and others concluded that a severe shortage of highly trained technological personnel had become a primary obstacle to Israel's future growth in the cyber realm and high tech generally, as well as to its rapidly expanding needs in the defense area. The resulting INCD strategy for the development of human resources in the cyber field, designed to expand the overall national pool of technological personnel, was based on a three-tiered pyramid of skills: at the bottom a broad-base of information and communications technology personnel generally, a second layer of more highly trained cyber specialists, including those in the defense area, and on top a smaller number of truly exceptional R&D experts, those who account for most of the important breakthroughs.[42]

To increase the national pool of technological personnel, three further decisions were made. The first was to begin educational programs in schools at as early an age as possible.[43] Research demonstrated that students who had studied computers in high school were far more likely to continue working in the field in the future, even if they did not serve in computer-related units in the IDF. Among those who did serve in such units, the numbers were even higher.[44]

The second decision was to make a special effort to reach out to population groups that were underrepresented in technological fields and which were likely to remain so in the absence of remedial efforts. A primary target audience in this regard was young people from rural and disadvantaged areas, known in Israel as the periphery, as well as women, ultra-Orthodox Jews, and Israeli Arabs.[45] To this day, despite the extensive programs outlined later, the high tech sector is still

[††] In its earlier incarnation as the INCB.

comprised of approximately two-thirds Jewish men, one-third Jewish women; only about 3% are ultra-Orthodox and 2% Arabs.[46]

The third decision was to enlist Israel's high tech sector and academic institutions in the effort to increase the overall national pool of cyber personnel. IDF training programs, impressive though they already were at the time, were insufficient to meet its own needs let alone to propel the entire ecosystem forward. Industry was found to be a particular bottleneck. Most cyber positions require three or more years of experience, but the costs of training new personnel on the job are very high. As a result, Israeli industry adds too few new people each year, despite the overall shortage in personnel.[47]

The INCD's well thought out human resources development strategy notwithstanding, the various cyber educational programs described later had their origins in a typically ad-hoc and informal but effective Israeli fashion. A few IDF officers and cyber executives, who knew each other, got together, identified the need, and began educational programs in a number of schools that were interested in participating. Unsurprisingly, the early programs focused primarily on the IDF's needs, especially mathematics, English, and programming.

Public School and Adult Education Programs—in 2016 the Ministry of Defence and INCD assumed formal responsibility for the programs and a national Cyber Education Center (CEC) was established. In addition to increasing the size of Israel's overall pool of cyber personnel, the CEC was charged with promoting social change through cyber education. Unlike the Ministry of Education, which is structured to address the needs of the school-age public as a whole, both in terms of the quality of teachers and level of instruction, the CEC was to hire advanced scientific and technological personnel in order to provide after-school programs and schools (even universities) with up-to-date pedagogical guidance and address the needs of exceptional young people.[48]

The CEC now oversees a range of cyber education programs, from the sixth grade through high school, all of which prepare students for future positions in high tech firms and academia, as well the IDF and intelligence agencies.[49] One such program, Shift, provides seventh graders with their first exposure to a variety of cyber related technologies, such as coding, algorithms, computer graphics, app programming, information security, and artificial intelligence. Outstanding middle school students (grades 7–9) can continue with a more in-depth after school program, StarTech, which includes training in programming, mobile apps, graphic design, computer games, and more, or with OnTop, a two-year problem solving and coding program.[50] The three-year Gvahim (Heights) program for grades 10–12 provides students with the opportunity to obtain a matriculation degree in cyber studies, computer science, or mathematics. At the time of the program's founding, Israel was the only country in the world to

offer high school students the opportunity to take matriculation exams in cyber studies.[51]

The highly competitive Magshimim (Dream Fulfillers) program provides university-level instruction in cyber studies to underprivileged high school student who have exceptional coding and hacking skills. Much like Gvahim, it initially started as an initiative of the IDF and a private foundation, but rapidly became a national program and is now offered in 25 different locales, with 142 active classes. Like Gvahim, Magshimim is for grades 10–12, but is an afterschool program. Classes meet twice a week for three hours and students further commit both to ten hours of homework each week and to participate each year in two cyber workshops and a summer cyber camp. In the late 2010s, approximately 700 out of 3,500 applicants passed the stringent entrance exams each year, of whom over 450 typically completed the program. 2,800 students will have graduated the Magshimim program by the end of 2022. The IDF and MoD share in the program's budget,[52] a clear indication of the importance they attach to it.

Participants in Magshimim have so outperformed their peers that the IDF asked that it be expanded to middle school students, as well. A further indication of the program's success is that more than 30% of Unit 8200's cyber personnel are Magshimim graduates today, in contrast with the even more highly disproportionate share of soldiers from socioeconomically well-off homes in the past. Some 65% of Magshimim graduates serve in intelligence and technological units, including cyber, and are avidly sought out by private sector firms upon completion of their military service.[53]

Another program, Gesharim ("Bridges"), is specifically designed for 7th to 9th graders from underprivileged communities. Run jointly by Unit 8200 and the IDF Educational Corps, the program provides training in coding, website and app development, cyber security and AI. In so doing, it also seeks to strengthen students problem-solving capabilities and sense of self-confidence and worth. User-friendly and experiential training programs, developed by Unit 8200, are used. The pilot program, which just began in 2022, has proven highly successful, with the heads of local authorities and parents pressing to have the program expanded to their communities. In 2023, it is expected to reach 18,000 students. [54]

Odyssey is a four-year program for exceptionally gifted students who wish to pursue an academic degree in computer science, or cyber studies, while still in high school. Many graduates subsequently enter the IDF's program for gifted soldiers, Talpiot (see below), and go on to become academic researchers and CTOs. Although Odyssey is small in numbers, just a few tens of students each year in each of the participating universities, it has an outsized impact.[55]

The CEC has put in place a number of projects designed to reach female, ultra-Orthodox, and disabled students. The CyberGirlz program provides a virtual community and mentoring program to attract young women interested in computer and cyber sciences. The mentors—all female—include soldiers in IDF technological units, college students studying computer science and software engineers and programmers from high tech companies. An earlier and now discontinued program, Mehamemet (Gorgeous), was also designed to encourage young women to pursue technological studies, providing 2,500 participants a year with their first chance to create an app.[56] Mamriot (Taking Off) trains Orthodox women for cyber and technological positions in the IDF, or as part of National Service (a non-military alternative to the IDF).[57]

The Ministry of Education, CEC, and some of the leading multinational R&D centers in Israel, cosponsor an annual "Coding Olympics" (dubbed "Skillz"), designed to encourage students to study coding and learn more about the cyber realm.[58] The Israeli branches of Microsoft, Google, and other leading tech firms conduct hackathons in which teams compete over the best means of preventing and mitigating simulated attacks.[59] Unit 8200 holds competitions in which students are challenged to disrupt an "adversary's" server, thereby enabling it to assess their performance and recruit the best among them.[60] Competitions such as these have been found to be an effective means of providing large numbers of young people with their first exposure to the world of programming. On-line courses for school age kids are another highly popular means of exposing them to programming and cyber generally.[61]

Between 2010 and 2023 the CEC will have spent approximately 250 million shekels[‡‡] on these programs, mostly for Magshimim. Of this, 90 million shekels will have come from a number of philanthropic foundations, the rest from the IDF, MoD, INCD, and other agencies.[62] Certainly by Israeli budgetary standards, these are impressively large sums.

Cyber security courses are now offered at every university in Israel, in addition to computer science and computer engineering.[63] A variety of non-academic adult cyber education programs are also available. She Codes seeks to increase the percentage of female programmers in the high-tech sector from the current 20% to 50%. Originally the initiative of a not-for-profit organization, the program soon gained government funding and now provides free training in coding for women in 40 centers around Israel. 4,000 women participated in the program in 2019 alone.[64] The Adva (Ripple) program, an unlikely joint endeavor of the Jerusalem municipality, tech giants such as IBM, Google, and Western Digital, religious seminaries, and philanthropic organizations, helps

[‡‡] In recent years the shekel has fluctuated between 3.1 to 3.5 to the dollar.

impoverished women from the ultra-orthodox community obtain undergraduate degrees in computer science and mathematics. Although still small, only 60–80 graduates in each of the program's first two years, it is considered a success and projected to grow rapidly.[65]

Rapid change is also underway among Israel's Arab population. Whereas there were a mere 350 Arab engineers in the high tech sector in 2008, of whom only a handful were women, by 2019 the number had skyrocketed to 6,600, of whom 25% were women. Between 1984 and 2014 only 50 Arab students, on average, obtained undergraduate degrees in high tech disciplines each year. In the 2018–2019 school year alone, 4,553 Arab students began academic studies in these areas. In 2022 the IIA began a $70 million five-year program to promote high-tech in the Arab sector[66].

Another program, Israel Tech Challenge, seeks to leverage Israel's image as a world leader in cyber and high tech to promote immigration of diaspora Jews. The program, which was funded by the INCD and run by the Jewish Agency, a semi-governmental body, connects applicants who have degrees from leading foreign universities, with potential employers in Israel, even before they arrive in Israel. To date, the program has succeeded in attracting hundreds of people specializing in data science and cyber security, mostly from the US and France.[67]

The IDF and Cyber Human Resources Development—compulsory military service is a primary source of Israel's high tech prowess and at the heart of the unique Israeli nexus of the IDF, academia, and industry. Compulsory military service enables the IDF to harness the talents of Israel's best and brightest, essentially for free, for a number of years and is viewed as nothing less than critical to Israel's cyber success, without which the IDF would not have access to most of them, who would be drawn into the private sector.[68] It also means that the total talent pool available to Unit 8200, for example, is unusually large, especially given Israel's otherwise diminutive size, 1,000–2,000 of Israel's very best each year.[69] Whereas the United States' NSA has approximately 40,000 personnel, Unit 8200 reportedly has as many as 10,000. This is significantly smaller than the NSA, of course, but not by orders of magnitude.[70] The deputy head of 8200 Uri Stav says that "the greatest present that we have is the high-quality personnel who get here every year. It is there inexperience and rapid turnover that contribute to rapid changes and rapid responses to changes in the environment. They grow up with a technology that is changing all time. They are less rigid and in many cases change come from below. . . Most of the unit changes professions every decade. . . We are in the process of transformation. . . We count on the fact that the veterans of computer, math and robotics olympics reach here, or related units, every year.[71]

A disproportionate number of these veterans then go on to found and/or run Israel's cyber security firms or become leading academic cyber experts.

Moreover, just a few geniuses play an outsized role and make all the difference in the cyber realm. Many of the IDF's top talents were already employed by high tech firms prior to their induction (at age 18), their skills are in great demand both by the multinational tech giants and Israeli firms and many would not have served had they not been required to do so.[72] The advantages of compulsory conscription come full circle at the end of soldiers' service, as well. Somewhere between a few hundred and approximately 1,000 top-notch cyber experts, the very best Israel has, are discharged from the IDF each year and join the ranks of Israeli industry and academia. These numbers are large even by international standards.[73] China's National Cyber Security School, for example, is scheduled to graduate a class of 1,300 students in 2022 and only plans on approximately doubling that at some indefinite point in the future.[74]

To find the very best and brightest, the IDF scours Israel's high schools long before graduates begin their military service and conducts intensive screening processes for the different units.[75] In practice, the IDF has a surplus of recruits who wish to serve in the cyber units today, including many who already have university degrees or work experience in leading tech firms. The IDF is thus able to focus on the top candidates in each age cohort and ultimately select the very best. The competition for these recruits among IDF units is fierce, with first pick going to Military Intelligence.[76] A former head of Unit 8200, now a high tech entrepreneur, puts it this way: "The biggest secret of the Israeli high tech system is the military's ability to look at people while they are (still) in high school." When combined with the hands-on experience they gain through military service, as well as Israel's cyber capabilities in academia and its high tech firms, the result, he believes, "sparks magic."[77]

One of the IDF's Talpiot program seeks out the top 2% of high school students each year. Only 10% of them pass the initial battery of tests, mostly in physics and mathematics, but even this select group is further winnowed down through two days of grueling personality and aptitude testing. Those accepted commit to serving in the IDF for at least nine years, during which time they pursue undergraduate and graduate degrees, undergo specialized military training, and are typically involved in major R&D projects, in such areas such as machine learning, data mining, programming, operating systems, communications networks, and information security. Approximately one-third of Talpiot participants choose to stay on in the IDF and pursue military careers, another third become academics, and many of the rest have gone on to become Israel's most successful high tech entrepreneurs.[78]

A new offshoot of Talpiot, Odem, was jointly launched in 2022 by the IDF, Mossad, and ISA, in conjunction with the Ministries of Defense and Education. The 12-year program, which begins in 10th grade with three years at a sleep-away high school, is followed by an undergraduate degree in electrical engineering

at the Technion and six years of service in IDF, Mossad, or ISA technological units. The program attracts participants by offering a free and personally tailored course of studies, with a large support staff, and assures them of "enormous influence" during their military service. Autonomous systems are a particular focus of the program.[79]

Unit 81's selection process is as grueling as Unit 8200's. Some 10,000 people meet the initial criteria each year and several thousand reach the screening process, but only a few hundred end up serving in Unit 81 or similar units.[80] The Academic Reserves (akin to the US ROTC) is still another source of exceptional personnel. Approximately 1% of high school graduates are given the opportunity each year to pursue undergraduate degrees in computer science, mathematics, engineering, and other areas of importance to the IDF, prior to their compulsory service. In exchange, they are required to serve for an extended period, typically five years.[81]

The IDF's critical need for highly trained and innovative personnel has made it one of the driving forces behind cyber education in Israel.[82] In addition to support for educational programs in the public school system, a variety of IDF units provide training programs that cover most areas of computer sciences, including mathematics, programming, infrastructure and network administration, software testing, and cyber defense.[83] Altogether, about 10,000 soldiers a year participate in these programs,[84] an indication of their subsequent impact on Israel's high tech sector generally.

Ever since 2012 the IDF has held a "cyber defenders" course, in which soldiers are taught how to analyze military computers and networks in order to detect and prevent attacks.[85] The IDF has also developed cyber simulators to train soldiers how to protect critical assets and networks.[86] In one course, soldiers train on a model Sim City, complete with residential and commercial neighborhoods, a railroad system, airport, electric grid, nuclear reactor, stock market, military base, and missile defense system. The simulated scenarios include cyber attacks that disrupt the cooling system at the nuclear reactor; remotely take over trains and traffic lights; shut-down the city's electric grid; disable the radar system at the airport; take control of stock exchange computers and cause a financial crisis; and hack the missile defense system to launch a direct missile at the city. Soldiers are trained to react quickly to prevent the attacks and are confronted with the consequences when they fail to do so.[87]

Approximately 500–600 soldiers are trained each year in offensive cyber operations at the Ashalim school in Beersheba. Courses typically last 20 weeks, starting with programming languages, before moving on to the specific skill sets the soldiers will need in their future units. Many have been glued to their keyboards since childhood, some already have undergraduate degrees when drafted and others have worked in high tech firms. High school or university

level courses in mathematics and computer studies are a prerequisite for admission in most cases.[88]

Of the trainees at Ashalim, 25–30% are graduates of Magshimim and on average 12.5% are women, a number that has grown over time. In an effort to encourage women, who have been found to perform better in less competitive learning styles, trainees at Ashalim are not allowed to compare their achievements with each other, but to their own past performance. In order to increase their capacity for self-criticism, trainees are encouraged to discover and correct their own mistakes on tests. They are also required to sign on for extra time in the IDF, beyond their compulsory service.[89]

The above programs have clearly had a positive, if still insufficient impact on drawing women into IDF cyber programs. Unit 8200, for example, has seen an increase from 5% to 25% in female officers at the level of captain to lieutenant colonel. The deputy head of the units is that "this is still far from the female potential. It is a problem at the national level and despite attempts to change it, the problem has not been resolved."[90]

IDF cyber training programs span the entire length of a soldier's compulsory service—and beyond. A highly select group participate each year in intensive pre-induction cyber courses, many of whom are then chosen to serve in the IDF's leading intelligence and technological units.[91] Prior to discharge, combat soldiers are offered the opportunity to participate in seven-week cyber immersion courses, designed to provide them with the skills needed to gain employment in the private cyber market.[92] A similar commercial course would last months and be very expensive, in many cases prohibitively so.

Another program, Maagalim ("Cycles"), provides pre-discharge combat soldiers with an even more intensive training course in Unit 8200. At the end of the program, half of the graduates then serve either in Unit 8200 or the C4I Branch, as regular (paid) personnel, for a period of up to two years. Some remain in the IDF, most are then discharged with highly attractive skills to the commercial market.[93]

One particularly innovative course, run by Intelligence Unit 9900, which is responsible for geospatial intelligence, including satellite and high-altitude surveillance images,[94] trains autistic soldiers to do the highly exacting work of image interpretation, a skill at which they have proven particularly adept. The program's success later led to the establishment of a cyber security training course for autistic soldiers, as well. A number of private firms support the program, providing professional mentors to train the soldiers and offering internships to graduates, potentially leading to long term employment.[95]

Another way in which the IDF contributes to Israel's high tech prowess is through the unusual professional experience and command responsibility that it provides soldiers at a very young age. At a time when many of their peers abroad

are still enjoying the final years of youth in college, these young soldiers are gaining real-world leadership experience commanding technological or combat units and/or learning advanced professional skills. Not everyone can serve in positions such as these, of course, but over half of the entire national population and nearly the entire secular Jewish population do serve in the IDF. At the very least, they are exposed to advanced military systems and to the IDF's innovative culture. It is an intense, transformative, and maturing experience, and the result is a workforce with an unusual number of highly trained, motivated, and disciplined young people with a can-do approach to problem-solving.[96]

In order to retain high quality cyber personnel, the IDF has been forced to be creative and devise special models of military service for them. One such model, known as "industrial capsules," enables cyber personnel to work in private firms for given periods of time and then return to military service. Another model allows IDF cyber personnel to work part time, while going to university, or working for private firms.[97] In addition to improved retainment rates—the primary objective—these models also provide the IDF with the benefit of the experience gained by personnel in the private sector, while the latter, which suffers from a constant shortage of highly trained cyber personnel, benefits as well.

An Innovative Cyber Culture: Chutzpah Gone Viral

Israeli society has a number of cultural attributes that make it particularly suited to high tech generally and to the cyber realm in particular. Start with a deeply ingrained national propensity to challenge authority and reject accepted norms, practices, and wisdom. Add a refusal to take no for an answer and constant search for alternative means of achieving an objective, even if it requires surmounting obstacles normally thought to be impassable. Further, add a belief that dedication, hard work, and out-of-the-box thinking can enable one to achieve almost any objective, along with a high tolerance for risk taking.[98] We call it chutzpah gone viral.

Drawing on Jewish traditions that emphasize knowledge and critical learning, including yeshiva education, in which students have long been encouraged to dispute interpretations of the Torah and other sacred texts, these national traits are also an outgrowth of Jewish history. Throughout the millennia, a sense of discrimination and persecution at the hands of hostile Gentile authorities imbued Jewish tradition with a view of authority, and of rules generally, as obstacles to be overcome, or circumvented, not constructive measures to be obeyed for the common good.[99]

Further contributing to the propensity to challenge authority, Israel is a highly heterogeneous immigrant society, with a population stemming from more than 70 different nationalities and cultural backgrounds. Israel may be predominantly Jewish (although approximately 20% of the population is not), but Jews of Iraqi, Polish, Ethiopian, Russian, or American heritage, for example, share little in the way of a common social and cultural background.[100] Each group has its own unique experiences, values, and ways of doing things, resulting in a constant state of social and cultural tension, often conflict, and a refusal to accept the norms and rules preferred by others. One of the results of this ongoing clash is an extraordinary degree of creativity.

Immigrants, by their very nature, are entrepreneurial risktakers and drivers of scientific and technological innovation who transfer new skills and knowledge to their adopted states and raise the standards in them. In Israel's early decades, many immigrants were also the hardy survivors of the Holocaust or of long-standing persecution in the Arab world. Others were pioneers, engaged in settling the land and in agriculture in highly adverse conditions, and still others came to Israel despite the opportunity to live a more secure and financially rewarding life elsewhere.[101] All were forced to be creative and seek innovative solutions in order to succeed.

Necessity may be the mother of invention but so too is adversity, whether at the individual or national level. Faced with severe threats to its security and even existence, especially in the early decades when Arab hostility was at its height, resources scarce, and institutional capabilities limited, Israel was forced to find creative ways to survive and build a new society nearly from scratch.[102] Moreover, the pace of change in Israel's environment, both external and internal, has been frenetic. Decision-making in Israel thus came to be all about immediate responses to military threats and staying alive to fight another day, while stitching together the resources needed through a variety of impromptu measures.

The result has been a marked capability to embrace and cope with change, an unusual propensity for improvisation, and a national decision-making style geared toward flexible responses to rapidly changing circumstances, rather than deliberate forethought and systematic planning. To a large extent, this was an unavoidable outgrowth of Israel's harsh external environment, but what began as a necessary evil has remained a primary characteristic of Israeli decision-making to this day, in both governmental and private sectors, indeed, it has become a national hallmark, sphere of excellence, and virtual faith.[103]

Israel's difficult and frenetic environment, further reinforced by the shared experience of military service, has produced a focused and pragmatic problem-solving orientation, and imbued its people with the ability to function comparatively effectively under conditions of high pressure and stress. These are

particularly valuable attributes in a field such as the cyber realm, in which the pace of technological development is extraordinary. As Gabi Siboni has noted "the United States has greater capabilities than Israel in cyber space, but we are small and very tense. It is like the difference between a speedboat and an aircraft carrier. We go very fast."[104]

Another view attributes Israel's high-tech success to the freewheeling and unregimented nature of Israeli childhoods, along with parents' greater tolerance for risk in child rearing. The unusual freedom Israeli children have to experiment and take chances, in the absence of strict social norms of behavior, is embedded in Israel's culture and institutions.[105]

Furthermore, and for reasons again having to do with the nature of its early years, Israel's national culture has always been non-hierarchal and informal to the extreme. The era of the kibbutz (agricultural commune) and socialism may be long gone, but the egalitarian norms established by the founders remain, and Israel has been aptly called a "relentlessly informal nation," or in more academic terms, a "small power distance society," in which formal hierarchy is paid little heed.[106] These national attributes are characteristic of the business culture typically found in R&D and high tech firms worldwide. Their informal and flat hierarchical structures and need for a free and open exchange of ideas, in pursuit of collaborative objectives, are highly reminiscent of kibbutz culture.

Israeli culture further combines a well-developed group orientation and willingness to act in pursuit of collective group goals with a strong sense of individualism.[107] Related to this, and again partly a function of Israel's strategic circumstances, is a greater willingness on the part of the governmental, private, and defense sectors to work together in far closer collaboration than is common in most other democracies.

IDF Culture and Cyber Innovation—in addition to the basic national characteristics described earlier, generations of IDF soldiers have been inculcated with the IDF's organizational culture, which emphasizes hard work, tenacity, dedication, professionalism, and team work, all under extremely challenging deadlines and circumstances.[108] Like other militaries, the IDF is highly mission oriented, but it differs in the emphasis it places on creativity and improvisation, no less than the formal authority stemming from rank or education.

IDF officers and even fresh recruits are encouraged to think creatively, out of the box, and to improvise in order to best achieve an objective, rather than mindlessly follow orders dictated from above, even when this means breaking rules. At least by the standards of military organizations, the IDF is informal, flexible, and non-hierarchical, with an unusual tolerance for dispute and risk-taking.[109] Indeed, IDF lore celebrates officers who take the initiative, improvise, and solve problems rather than going by the book. Officers who fail to improvise are commonly perceived as lacking initiative, self-confidence, and resolve. This

unorthodox military culture is further reinforced by the ubiquitous presence of reservists, who have little regard for rank, throughout IDF units and echelons.[110]

IDF officers, at all levels, are expected to express their views forcefully when they disagree with superiors and to continue to do so until a final decision is made. Junior officers are expected to press their case with their superiors and senior officers with the chief of staff, who is in turn expected to press his case with the prime minister.[111] Little illustrates this better than the following scene, which took place in the White House just minutes before the signing of the Oslo Accord in 1993, as described by one of the Americans present:

> The commander of the IDF Central Command, Ilan Biran, entered President Clinton's office and launched into a stormy debate with Prime Minister Rabin. The commander argued that Rabin must not agree to the new deployment lines . . . Rabin embarked on a long, vociferous debate with the general, while the rest of us, including the president, had to wait . . . We were astonished. In our wildest dreams we could not have imagined that such a situation would occur between a premier and one of his generals. And all this at the White House, in front of the president.[112]

Unit 8200's organizational culture is reported to resemble that of a startup, and challenges to authority are encouraged. "We teach them how to work out of the box," according to a former senior officer.[113] Unit 81 is even more extreme. Most soldiers in the unit do not wear uniforms, the base does not look like a military installation, and veterans refer to a sense of freedom, "balagan" (chaos), and an emphasis on knowledge and charisma, as opposed to rank.[114]

Unit 81 is essentially a sub-contractor for the intelligence community. The assignments given to it typically appear impossible at the outset, but some veterans view them as the source of their success in later civilian life.[115] According to one veteran:

> What we essentially do each time is establish a startup . . . We solve a problem with a limited budget and at all hours of the day . . . with the understanding that people's lives are at stake. You have one opportunity and can't fail . . . The (unit's) motto[§§] may sound like a slogan, but it is true—if you truly understand a problem and the limitations, you can solve anything. Later on in the business world, it changes the way you

[§§] "Turning the impossible into the possible."

> look at matters . . . and the importance of providing a precise solution to the requirements and testing to make sure that it works consistently.[116]

Yigal Unna, a former head of the INCD, stresses that the IDF gives soldiers "a license not only to do interesting things for the state in the cyber arena, but also trains them for one thing: not to be afraid, to try, to take risks, to experience failure."[117] The officer in charge of the IDF's cyber defenders course states that soldiers are taught "to think differently, to search for things that are less visible, in the places where one does not usually look. They have to search for things on the Internet that people have tried really hard to hide. If we just search like everyone else, we won't find them."[118] A former commander of Unit 81 described its recruitment and training programs in similar terms:

> When the soldiers are recruited the emphasis is not necessarily on their knowledge of computers or electronics. We are looking for people who can think outside the box, but who can also collaborate with others who have similar traits . . . we don't ask candidates to write code, instead we give them a complex problem to solve in order to examine how they come up with a solution.[119]

The shared military experience further engenders a strong sense of group cohesion and a desire to continue working together in civilian life, one of the reasons so many high tech firms in Israel have been established and staffed by veterans of units such as 8200 and 81. After leaving Unit 81, according to one veteran, "you realize that up to that time you did the wildest things in your life together with the most talented people and you want to extend that into civilian life." A former commander of Unit 81 observes that soldiers still doing their compulsory service "see veterans doing well and don't want to become salaried developers, but to blaze new paths, because that was the drive that was instilled in them."[120]

Units 8200 and 81 may be unusual, but they do reflect something unique about the IDF in general. In any event, the willingness to challenge authority and conceptual orthodoxies, internalized prior to and during military service, has a direct impact on Israel's civil high tech world.[121]

Social Networks

Social networks, domestic and international, are important determinants of scientific and technological achievement. Social networks can provide information about a variety of critical areas more efficiently than markets or governments, including scientific and technological developments, job opportunities, and ties

to skilled applicants. They can further match entrepreneurs and investors who might otherwise not find one another and help find business opportunities for highly specialized high tech products. In so doing, social networks drastically reduce the costs and risks of innovation.[122]

Social networks are especially important sources of information about geographically removed opportunities, of particular importance for Israel given its distance from international markets. To this day, but especially in the 1980s when its high tech sector was still in its infancy, Israel has built networks linking Jewish businesspeople and financiers in the United States with high tech startups in Israel. A further international network was formed by immigrants from scientifically and technologically advanced countries, whether from the West or especially Russia during the 1970s and 1990s.[123] Diasporas are particularly efficient networks for connecting people and exchanging information and knowledge required for innovation.[124]

Clusters are a particular form of social network. Clusters produce valuable exchanges of information that help firms become more competitive, provide skilled labor and economies of scale, attract FDI, and have a variety of valuable assets, including technology, skills, and information about markets and customer needs. Clusters are at their best when they allow scientific and technological personnel to move easily between firms or create spinoffs and startups of their own. Universities and research institutes are often essential players in clusters.[125]

Israel remains a small country, with a population that is now similar in size to that of New York City, Switzerland, or Austria. The old Israeli truism, whereby "everyone knows everyone" whether from high school, military service, or university, is no longer quite true, but is not off by that much. The technological expert whose advice one seeks is usually no more than a phone call away[126] and national decision-makers are typically at a distance of no more than two degrees of separation. There may be a number of identifiable high tech hubs, but the physical distances are small and in practice all of Israel, between Haifa and Beersheba, really constitutes one long cluster—a "Silicon Wadi." The result is an easily accessible wealth of expertise and ease of communication that greatly facilitates R&D processes in Israel.

Virtually everyone in Israel's high tech sector has served in the IDF, many in the technological or combat units. When combined with the nation's small population and geographic size, the result is a comparatively close relationship between the government, IDF, academia, and high tech sector. Reservists, in particular, serve as a conduit and bridge between them.[127] Reservists gain firsthand exposure to the IDF's operational needs and shortfalls and thus the ability to propose ideas for new or improved capabilities. Many reservists also have close ties to decision-makers at senior business and national levels, thereby greatly reducing the time between the identification of a need and development

of the necessary response. Reservists further form an important network for exchanges of professional and social information and for recruitment purposes, matching the needs and skills of employers and employees.[128]

The opportunity to maintain connections with peers, former commanders, and reservists helps create a highly developed networking system for business, employment opportunities, and social purposes. A single individual's military service can yield hundreds of ties on various levels and with people of diverse localities and socioeconomic backgrounds.[129] Some headhunting firms specialize exclusively in veterans of Unit 8200 and/or other technological units in the military. Unit 8200 itself has an alumni association of 15,000 veterans, which hosts a variety of networking events designed to help members find appropriate employment in the R&D sector and to promote business opportunities. Unit 81's alumni association has 5,400 members and conducts various programs designed to develop entrepreneurial skills, help those interested in entering the entrepreneurial world, and promote entrepreneurial endeavors. Unit 9900 has a similar network.[130]

Veterans of Unit 81, for example, tend to recruit their former subordinates and teammates when launching startups. They in turn leave these firms to found startups of their own, recruiting people discharged more recently from military service, and creating a repetitive cycle. Indeed, it is not rare for firms to be founded by teams comprised entirely of Unit 81 veterans. The networking benefits do not end with the founding of firms or recruitment and mentoring of newly discharged comrades. Younger veterans commonly raise capital from their predecessors in an informal angel circuit.[131] Veterans of Unit 8200 and other high tech units act in similar ways.

Clouds, Possible Misdeeds, and New Opportunities

Israel's many achievements in the high tech and cyber areas notwithstanding, it faces a number of difficult challenges in the coming years. With a small population base to draw on, a shortage of computer scientists, engineers, and other highly skilled professionals has become a major obstacle to further expansion of Israel's high tech sector, especially in the cyber realm. By the mid-2020s, it has been estimated that Israel will face a shortage of approximately 10,000 engineers and programmers in a market that currently employs 140,000.[132] In 2019 Israel already suffered from an overall shortage of 18,500 tech workers (engineers, programmers, and others)[133] and in the cyber realm alone a shortage of some 20% of the personnel needed.[134] Competition with global giants such as

Facebook, Google, and Microsoft, which offer especially lucrative employment packages, makes the competition for highly skilled personnel particularly fierce.

At present, the high tech sector is still benefiting from the major strides made by Israel's educational system in earlier decades. In the coming years, however, the ongoing deterioration of the educational system that has taken place in more recent decades, at all levels, will presumably have a growing impact.[135] In 2020, the head of the National Council for R&D warned that Israel may lose its leading place in innovation and high tech by 2030 if it does not greatly increase funding for academic R&D. On paper, Israel invests a great deal in R&D, per capita, especially compared to Europe, but 85% of Israeli R&D, he argues, is actually conducted in the R&D centers established by the multinational corporations, while government funding for academic R&D is now among the lowest in Europe. Whereas the budget of the Israel Innovation Authority equaled 1% of the state budget in the early 2000s, it constituted less than 0.5% in 2020, admittedly of a much larger state budget; the EU, United States, and South Korea devote between 0.6–1% of their GDPs to innovation, Israel now devotes only 0.15%. The multinationals follow the human resources, and if they conclude that there are better opportunities in other countries, R&D investment in Israel may dry up rapidly.[136]

Contrary to the public image, emigration from Israel is low, especially for an immigrant society, indeed, lower than the OECD average,[137] and has decreased steadily over time. Even among highly qualified native-born Israelis, emigration is just above the OECD average.[138] Conversely, the quality of the human capital lost is high and Israel is suffering from an ongoing brain drain. In 2015, 5.6% of all Israelis who had received undergraduate or graduate degrees between 1980 and 2009, in any field, had lived abroad for three or more years. The problem was particularly acute among PhDs, of whom 11% had lived abroad for three or more years, and especially so among those with PhDs in mathematics (25%), computer science, aeronautical engineering, biology, chemistry, physics, and genetics (each between 16–18%).[139] Obviously, the three-year cutoff point is arbitrary, and many will ultimately return, but it provides a clear indication of a worrisome trend for Israel.[140]

Given the growing shortage of high tech personnel, Israeli firms are increasingly setting up R&D facilities off shore, with Ukraine, Russia, and India the most popular sites.[141] In 2017, for the first time, the government was forced to approve the hiring of 500 foreign high tech workers. Plans were also announced that year for a 40% increase in the number of computer science graduates over five years, at a cost of some 700 million shekels. In 2018, in an indication that the five-year plan was beginning to pay off, and for the first time in Israel's history, more students registered for engineering than for any other academic discipline. Together with computer science, mathematics, and statistics, they accounted for

approximately one-quarter of all university students in Israel. In early 2022, in a further indication of the five-year plan's success, the National Economic Council found that the number of students in the high tech disciplines had actually increased by 50% and forecast that this would continue to grow by an impressive 40% to a whopping 25% by 2030. Favorable demographic trends, especially the rapid growth of Israel's young secular population, the primary source of high-tech personnel, and an increase in the number of high school students studying advanced mathematics, were among the reasons for the more optimistic assessment.[142]

The success in bringing new companies to the ATP in Beersheba in the early years notwithstanding, the city's geographic distance from the center of the country has proven a major stumbling block, and the pace of expansion has slowed. Even relocation of IDF intelligence units has been postponed indefinitely due to internal resistance. The government plans on launching a number of new programs to help promote the ATP, but its stated objective of reaching 10,000 high tech employees in Beersheba by 2025, not including IDF personnel, appears ambitious.[143]

Although the overall number of cyber firms in Israel doubled between 2014 and 2019 and the total value of venture capital raised by the cyber sector, as well as cyber IPOs, have grown steadily, the rate of growth has slowed significantly, and Israel's cyber industry appears to be maturing. Whereas 86 new cyber firms were established in 2015, only 70 were established in 2017, 42 in 2018, and just 12 in 2019. The number of new multinational R&D centers established in Israel has similarly slowed, from 40 in 2015 to 23 in 2019 and just 4 in 2020. This decrease mirrors the slowdown in the high tech sector as a whole, from 1,400 new startups established in 2014 to just 520 in 2020.[144]

One study found two primary reasons for the dramatic decrease in the overall number of high-tech startups in Israel. The first reason, which accounts for most of the change, is typical of the global high-tech arena as a whole. Whereas advertising and social media had been the primary engines behind the establishment of new startups between 2010 and 2014, following the advent of smart phones, changes in technology, market forces, and governmental regulation led to a drop in the number of new startups in these areas. The second, more Israel-centric reason, has to do with the rapid increase in the number of global corporations operating in Israel, approximately 200 during the same 2010–2014 period. These corporations offer highly attractive, low risk compensation packages, thereby reducing the motivation to establish new start-ups.[145]

Israel has, therefore, decided to invest heavily in what it believes will be the next major realm of innovation, AI. In an effort to replicate the successful model that led to Israel's cyber revolution, a special task force was established to propose a national AI strategy, once again with the participation of the government,

IDF and defense establishment, academia, and the high tech industry. The task force submitted its recommendations in 2020. Much as its cyber predecessor had done years earlier, the AI task force recommended that Israel seek to become one of the five global leaders in the field within five years. Israel is already thought to be in third place in the number of AI related firms, after the United States and China, and sixth in leading AI scientists.[146] The task force further recommended that a special body, akin to the INCD, be established to lead and coordinate all national efforts in the AI area and that a budget of some 10 billion shekels be allocated over five years.[147]

In the field of quantum computing, in contrast with AI, a special committee recommended in 2020 that Israel only seek to become a "threshold state," given the magnitude of the investment required to become a world leader. Nevertheless, the government allocated 1.25 billion shekels for a five-year National Quantum Initiative, largely to develop the necessary human resources, as well as 200 million shekels to build a foreign-made quantum computer in Israel, which was to constitute the basis for the future construction of an Israeli-made one. The defense establishment, which attributes strategic importance to quantum computing, is deeply concerned that states that do not have their own independent capabilities in this field may not be able to purchase them abroad. It is thus heavily involved in the initiative.[148]

Software sold by Israeli companies is currently believed to be in use in roughly 130 states.[149] Over and above their commercial value, a significant consideration for all states, these sales have also become an important part of Israel's efforts to build relations with foreign partners, including those with which it did not previously enjoy diplomatic ties. This has been particularly true of a number of Arab states, which have overcome their historic hostility and established commercial and even formal diplomatic ties with Israel, at least partially in order to gain access to its high tech and cyber technology.[150] For diplomatically challenged Israel, this new form of "cyber diplomacy" has become an important instrument of foreign policy. It paid off particularly handsomely in the decision of Bahrain and especially the UAE to sign peace agreements and establish diplomatic relations in 2020, which have been greatly expanded in a variety of areas ever since (see Chapter 9).

In the past, Israel restricted cyber exports to defensive software, banning offensive sales, a highly ambiguous distinction in the cyber realm.[151] In effect, it left it up to the exporters to make the distinction, a clearly unsatisfactory situation. Israel subsequently began also approving sales of offensive software, leading to more criticism from various human rights groups, multinational corporations, and others who argued that the country was already too lenient and demanded that Israel adopt tighter controls. Israeli firms, conversely, contended that governmental export controls were stricter than those in most other countries and

placed them at a competitive disadvantage.[152] One government official put the dilemma this way: were Israel to increase oversight too much, these firms would simply move to Cyprus or Macedonia, and it would lose both the firms themselves and the ability to supervise their exports.[153]

A key component of Israel's export laws revolves around the Wassenaar Arrangement, a nonbinding international arrangement between 42 nations that regulates the export of dual-use technologies, including cyber. Inclusion of a technology on the Wassenaar Arrangement "control lists" does not constitute a ban or prohibition on its export but is a commitment by the participating state to require that sales be governed by its national export control policy and licensing requirements. Most of the member states, including those from the EU, have added certain surveillance and intrusion software to the regulated items. The US position, in contrast, remains to be resolved, due to ongoing concerns regarding the differentiation between offensive and defensive uses. Israel is not a party to the Wassenaar Arrangement but adheres to its guidelines and has passed laws adopting them.[154]

This ambiguity between offensive and defensive uses has led to some troubling outcomes in Israel's case. Cyber tools from Israel have been exported to authoritarian regimes, which have reportedly used them to target journalists, dissidents, human rights activists, and others. Two firms, in particular, have been the focus of attention, the NSO Group and Verint, both of which maintain that they sell spyware only to governmental clients and solely for purposes of counter terrorism and crime prevention. Their clients, however, include noted human rights violators, such as Saudi Arabia, Azerbaijan, Mexico, the United Arab Emirates, Qatar, Bahrain, South Sudan, Indonesia, and more.[155]

In 2021–2022 NSO became the focus of a global scandal, with ramifications for Israel's international standing and use of cyber as an instrument of diplomacy. Seventeen media organizations, including the *Washington Post*, the *Guardian*, *Le Monde*, and *Haaretz* joined together with Amnesty International and a French media nonprofit to form the "Pegasus Project," an international investigative consortium named after NSO's premier product. In a series of detailed reports, blasted over a number of consecutive days on the consortium members' front pages, as well as by other leading news media around the world, such as the *New York Times*, the Pegasus Project presented a dramatic picture of alleged abuses by NSO and other Israeli cyber firms. The fact that NSO, according to the *Washington Post* and others, is just one of a number of major firms in its field further accentuated the unique attention afforded to it.

The consortium found that 189 journalists, dissidents, human rights activists, politicians, and heads of state, in 21 countries had been identified as possible targets of surveillance by at least 12 NSO client-governments, and that this surveillance had actually been carried out in a number of cases. Those targeted

came from a list of over 50,000 phone numbers from approximately 50 countries, which may have been noted as subjects of interest and considered for surveillance by NSO clients. The consortium was able to identify more than 1,000 people on the list, including six sitting presidents and premiers (in France, Iraq, South Africa, Pakistan, Egypt, and Morocco), seven former premiers (France, Belgium, Yemen, Lebanon, Algeria, Uganda, and Kazakhstan), and the King of Morocco. Also on the list were the phone numbers of the wife and fiancé of murdered Saudi journalist Khashoggi and a prominent Mexican reporter who was gunned down on the street, indicating the possibility of indirect NSO culpability. The phones of 11 US diplomats serving in Uganda were also hacked using Pegasus.[156]

NSO's close ties to the Israeli government and the allegation that it had provided the government with at least some of the intelligence collected were particularly damaging. In some cases, such as India and Hungary, NSO clients reportedly started using Pegasus just a short time after state visits by Prime Minister Netanyahu and possibly as a direct result. Moreover, the MoD was reportedly involved in selecting, sponsoring, and in some cases even initiating the first contacts with NSO clients, including active encouragement of ties with the UAE, Bahrain, and Saudi Arabia, even after the Khashoggi scandal erupted. The government reportedly also encouraged a number of other Israeli cyber firms*** to work with Saudi Arabia and other clients.[157]

Following the revelations, a number of states, including the United States, UK, France, Canada and Australia as well as the EU and leading multinational firms, such as Apple and WhatsApp (which is owned by Facebook), expressed concern about Israeli cyber sales to authoritarian regimes. The United States ultimately blacklisted NSO and Candiru, another one of the Israeli firms, from receiving exports from US firms,[158] even though critical US security agencies had actually either bought Pegasus or considered doing so. The CIA, for example, bought Pegasus on behalf of the government of Djibouti, for counterterrorism purposes, despite long-standing concerns regarding human rights abuses. The FBI bought it for possible use in criminal investigations, but claimed that it had merely evaluated the program and decided in the end not to make use of it, while the DEA found Pegasus too expensive. The Secret Service and US Africa command held discussions with NSO regarding Pegasus.[159]

These incidents and others have led a number of human rights groups, as well as Microsoft, Facebook, and others, to call upon Israel to more tightly regulate its cyber exports and in NSO's case ban them completely. Even before the Pegasus Project scandal erupted, Amnesty International, Facebook, and 50 other entities

*** Verint, Candiru, Quadream, and Cellebrite.

had filed suit against NSO and the Defense Ministry, arguing that Israel had failed to meet its duty to halt exports when evidence of harm existed.[160]

Approximately half a year after the international scandal, a domestic uproar erupted in Israel over reports that the police had made unauthorized use of Pegasus against some two dozen prominent Israelis. The police were accused of either bypassing judicial oversight altogether or of deploying spyware from NSO and other firms in a manner that exceeded the parameters set by the courts. A government inquiry subsequently found that the police had only actually exceeded the court orders in one, possibly two, cases and that no use had been made of the information collected.[161] The brief uproar, nevertheless, brought the dangers of unbridled use of spyware of this sort home to the Israeli public, turning it from a foreign policy issue to one with domestic ramifications as well.

Under the combined weight of the scandals, domestic and international, NSO, and a number of other companies encountered growing financial difficulties, A number closed entirely and NSO downsized significantly. Its long-time founder and CEO was forced to resign.[162]

Even before the NSO scandal, the government had begun responding to the conflicting commercial, diplomatic, and legal needs, streamlining the export approval process but also adopting measures to ensure greater oversight.[163] One key component was shortening the length of time it takes Israeli firms to go through the rigorous export license process from the commercially untenable year or longer to a few months.[164] Conversely, a new division was to be established in the Ministry of Economy and Industry to strengthen oversight of exports of cyber technologies with civilian applications and to complement the already existing mechanism in the MoD, which is responsible for oversight of security related exports. The MoD cut the number of states eligible to buy offensive cyber exports from 102 to 37, mainly the United States, Canada, the EU, Japan, India, Australia, and New Zealand. Saudi Arabia, the UAE, Morocco, and Mexico were no longer included. Sales were to be limited to governmental customers and to be used solely for purposes of the investigation and prevention of terrorism and severe crimes. The definition of terrorism and severe crimes was explicated, to prevent misuse, and legal sanctions were established for violations of the export controls, which were based on the "Wassenaar agreement." The new export controls also specifically defined those uses which would be proscribed, including those that might cause damage to people on the basis of religion, gender, race, national origin, and political and sexual orientation. The IDF began exempting reservists who work for firms engaged in offensive cyber tools from reserve duty, thereby reducing the danger of them being exposed to highly sophisticated new capabilities.[165]

Israel is not the only country trying to figure out how to deal with the benefits and dangers posed by cyber exports. The United States, UK, and other nations

play a big role in these markets and are struggling with similar issues. For instance, even though the United States is a signatory to the Wassenaar Arrangement, it has been slow to modify its export laws to become compliant, whereas Israel did so in 2013.[166] In addition, US, British, German, Italian, Austrian, and Greek firms have engaged in behaviors similar to NSO and Candiru, including sales to some of the same problematic states as Saudi Arabia, the UAE, China, and Belarus. In some cases, former members of the US national security establishment were employed by these firms and, much as in the case of the sales by Israeli firms, allegedly targeted human rights activists, journalists, and political rivals.[167]

9

International Cyber Cooperation

The big news is we're going global. The same national network that is working so well at the national level, we're opening up, announcing a global cyber net shield . . . because the main thing is, if you try to fight alone, you are going to lose. If you fight together, you are going to win.

Prime Minister Bennett

Part of our mission is to help improve the global cyber security area, because cyber is a lot like a biological pandemic—it spreads between countries regardless of borders and ethnicity.

Yigal Unna, Head of the INCD

Israel engages in cyber cooperation with approximately 90 states today, more than it has embassies in, and has signed formal cooperation agreements with some 30.[1] One hundred and fifty foreign delegations visited the CERT-IL facility in Beersheba in 2019.[2] As set forth in the relevant cabinet decisions and INCD Strategy, cooperation with other actors active in the cyber realm is an important component of Israel's cyber strategy. Indeed, the cyber realm has come to be perceived as an area in which Israel can strengthen not only its commercial and military capabilities but its foreign policy and soft power as well.

The importance of international law in the cyber realm, as in other areas, is also growing. Constructivist scholars believe that international norms, agreements, and law are necessary to restrain state behavior and build robust cyber security, especially since states do not enjoy a monopoly over force in the cyber realm.[3] Others are more skeptical and deem it unlikely that a binding international set of laws or treaties will arise and believe that the power of norms to constrain state behavior will prove even more elusive in the cyber realm than in the physical. Their skepticism stems, in part, from the ongoing dispute among states regarding the applicability of existing international law to the cyber realm, the absence of a global system of governance or international body truly capable of overseeing the implementation of international law in the cyber realm, and the reluctance of

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0010

states to craft binding agreements that will constrain their ability to use the cyber realm, a new and emerging realm, in support of their national interests.[4]

Chapter 9 has four sections. The first presents Israel's bilateral and multilateral cyber cooperation with a variety of partners. The second section provides a brief overview of the salient aspects of international cyber norms, law, and agreements, as the basis for understanding the third section, which presents Israel's involvement and policy in this area. The chapter concludes with a few observations regarding Israeli policy and praxis regarding international cyber cooperation and law.

Bilateral and Multilateral Cyber Cooperation

In the cyber realm, according to Prof. Eviatar Matania, a former head of the INCD, "no one will be able to do it alone." Israel thus "believes in sharing information between companies, sectors and countries because the threat is so global . . . The more countries are enabled, the safer humanity is in this new space."[5] International cooperation is also a means to compensate for Israel's limited independent resources and lack of global intelligence reach, a key characteristic of other top cyber powers and part of its effort to establish itself as one.[6]

In 2021 this approach toward international cooperation reached new heights with the announcement by Prime Minister Bennett that Israel was inviting like-minded states to join together in a "global cyber defense shield" modeled on the INCD. By sharing real-time, online information and alerts to identify cyber threats, conducting joint investigations, and pooling other resources, the new network is designed to help participant-states effectively address threats far more rapidly than they could on their own. Israel's already existing ties and cyber cooperation agreements with other states are to serve as the basis for the new network, which is designed to take cooperation to a new level.[7]

With the partial exception of the section on the US, with which cyber cooperation is extensive, and to a far lesser extent the UK and China, the publicly available information regarding Israeli cooperation with other partner states is both limited and often rather technical in nature, making a uniform presentation format, for each of the partner countries, unfeasible. In the interests of completeness, we present essentially all of the information available, as is.

United States—the US and Israel are two of the leading powers in the cyber realm but are also among the countries subject to the greatest number of cyber attacks. It is thus hardly surprising that in the cyber realm, as in essentially all other areas, the US is Israel's primary partner and the two states engage in extensive cooperation at the national security, civil, and commercial levels.

The height of formal US-Israeli cyber cooperation, to date, was in 2016, with the signing of three new agreements. The first, the "United States-Israel Advanced Research Partnership Act," added cyber security to an already existing bilateral R&D program run by the US Department of Homeland Security (DHS) and Israel's Ministry of Public Security. The act was designed to help firms overcome the critical stage between initial research and successful product commercialization.[8]

The second agreement, the "Cyber Defense Cooperation Agreement," between the DHS and INCD, provided for automated bilateral cyber defense programs, including establishment of new links and procedures between the two countries' respective Computer Emergency Response Teams (CERTs). Under the agreement, Israel became one of the first countries to join the DHS Automated Indicator Sharing initiative, which enables autonomous exchanges of cyber defense and intelligence. Given the rapidly changing nature of cyber threats, autonomous exchanges are essential and the US hopes that the initiative will ultimately evolve into an international coalition of dozens of countries. The agreement also provides for joint efforts to protect critical infrastructure against cyber attacks, manage cyber events, build partnerships in the private sector, and promote private sector cyber R&D.[9]

The third agreement was between the US Secretary of Defense and Israeli Minister of Defense and provided for heightened cyber cooperation between the two defense establishments.[10] Further details are unknown.

In 2016 the House of Representatives also passed the "United States-Israel Cybersecurity Cooperation Enhancement Act," which would have created closer links between DHS and the Ministry of Public Security, but it was never approved by the Senate. In 2021 the bill was submitted to Congress once again.[11] If approved, it would provide grants to promote cooperation between US and Israeli firms, not-for-profit organizations, academic institutions, and national laboratories and other governmental agencies on non-classified projects in two areas: commercialization of cyber security technology and joint cyber security R&D projects, with a particular focus on detection and prevention of cyber threats.[12]

The director of the US National Security Agency reportedly visited Israel in 2016 to discuss cyber defense cooperation with counterparts in Unit 8200, with a particular emphasis on countering attacks by Iran and Hezbollah.[13] There is no public record of further senior visits of this nature, in either direction, but it is hard to imagine that they have not been ongoing. US Cyber Command, the FBI, and the Department of Energy have cyber liaison officers in Israel.[14]

In 2017 bilateral cyber cooperation was formally raised to a new level, with the establishment of the US-Israel Cyber Working Group, headed by the White House Cyber Security Coordinator and the head of the INCD. The working

group was to have focused on preventive strategies to identify cyber adversaries before they threatened critical infrastructure,[15] an area of particular concern to both sides, but the subsequent decision by the Trump administration to eliminate the position of the White House Cyber Security Coordinator left the group in limbo.[16] New bilateral cyber security working groups were established in 2021 by the Biden administration.[17] Their work will presumably be facilitated by the appointments of a new cyber director in the White House and, for the first time, a national US "cyber czar,"[18] thereby providing heretofore missing points of contact on the US side for the head of the INCD.

In 2021 the US Department of the Treasury announced a partnership with Israel to counter the threat of ransomware. To this end, a joint task force was to be established and a Memorandum of Understanding signed, to support information sharing related to the financial sector, including cyber security regulations and threat intelligence. In 2022 the US Treasury and Israel's Ministry of Finance signed a further MoU dealing with finance-related cyber cooperation, in this case protection of critical financial infrastructure and emerging technologies. The agreement includes sharing of information, including cyber security regulations and guidance, cyber security incidents and threat intelligence; mutual staff training and sharing of methodologies to strengthen financial institutions' cyber resilience; and competency building activities, including joint cross-border cyber-financial exercises. A joint task force would provide for exchanges between technical experts on policy, regulation and outreach to support innovations designed to strengthen cyber-financial security and advance global compliance with international standards on money-laundering and counterterrorist financing.[19]

In 2022 the bilateral "Jerusalem Declaration" provided for increased collaboration in a variety of tech-related areas, including an "operational cyber exchange" and combatting cybercrime. To operationalize the doctrine, a very high level strategic dialogue on technological cooperation was convened.[20] In 2022, DHS signed five new cyber security cooperation agreements with Israel. The first, in the area of terrorist financing, focused primarily on ransomware and securing critical infrastructure and was to be a complementary agreement to the Department of the Treasury's partnership with Israel. The second dealt with cyber R&D and the third, signed by the Transportation Security Administration, part of DHS, focused on cyber security issues regarding air and ground transportation, including information sharing, joint exercises, and R&D. The fourth agreement provided funding for collaborative projects between US and Israeli firms and research institutions, designed to strengthen infrastructure resilience by promoting innovative technologies in the following areas: secure architecture for protecting core operational processes; real-time risk assessment solutions for small-to-medium-sized airports[21] or seaports; resilience center pilots for small

and medium-size businesses; and advanced data fusion and analytics. In a related agreement, DHS and the INCD joined together with the Israel-US Binational Industrial Research and Development Foundation (BIRD) to promote startups and projects in these areas, with the Foundation providing up to $1.5 million per project or 50% of the R&D budgets required. In addition to these agreements, the US and Israel were expected to undertake expert exchanges in a number of cutting-edge fields, including AI, quantum computing, and position navigation and timing.[22]

In 2021 President Biden signed a federal cybersecurity executive order of critical importance for Israel. The executive order opens new US federal cybersecurity contracts to foreign companies estimated to be worth $200 billion.[23] For security reasons, including lingering American mistrust stemming from past Israeli espionage (the 1987 "Pollard affair"), Israeli firms had been largely shut out of federal cyber security contracts. In contrast, Israeli participation in weapons development and manufacturing contracts has been extensive.

The US and Israel have also engaged in operational cooperation in the cyber realm. In 2020 tens of Israeli cyber defenders from the C4I Branch, Military Intelligence, IAF, and Israeli Navy, participated in "Cyber Dome," a cyber exercise simulating hostile attempts to cripple military operations. In the 2020 exercise, the fourth of its kind held in the US, American and Israeli forces reportedly acted as a "joint organic defense team."[24] In 2021 five teams of IDF cyber defenders were among 57 teams, from 14 countries, that participated in a US Army cyber exercise.[25] Israel provided the US with advanced warning regarding attempts to hack American power plants.[26] According to numerous sources, the US and Israel have also engaged in extensive cooperation in the offensive cyber realm, the most prominent case being the Stuxnet virus. Stuxnet and other examples of purported joint cyber attacks are presented in Chapter 10.

Some have raised the possibility that Israel might seek a US cyber guarantee,[27] possibly akin to the language of the standalone 1998 bilateral missile defense MoU, or even as part of a broader bilateral defense treaty. The missile defense MoU states that "the United States government would view with particular gravity direct threats to Israel's security arising from the regional deployment of ballistic missiles of intermediate range or greater. In the event of such a threat, the United States government would consult promptly with the Government of Israel with respect to what support, diplomatic or otherwise, or assistance, it can lend to Israel."[28] Alternatively the language might be similar to the 1958 US-UK nuclear agreement, which requires both sides to be "prepared to meet the contingencies of atomic warfare."

Israeli defense officials are cautious regarding the need to further expand and formalize military cyber cooperation with the US. Unlike most other military domains, in which Israel is heavily or entirely dependent on the US for

major weapons platforms, for example, combat aircraft, Israel is a global leader in the cyber realm in its own right, with independent capabilities that draw on its own national cyber ecosystem. There thus appears to be strong support for further expansion of military cyber cooperation, but also broad agreement that Israel should take care not to enter into cooperative arrangements that might risk exposing its unique capabilities, offensive and defensive, and constrain its freedom to act independently in the cyber realm.[29] These conflicting considerations clearly demonstrate an awareness of the need to balance the fundamental principle of assuring major power support, enshrined in Israel's strategic culture (see Chapter 6), along with the similarly critical, but partly conflicting, principle of self-reliance.

The extensive commercial ties between the US and Israel in the cyber realm are fueled by an ongoing exchange of funding, expertise, and people, which helps drive general high-tech innovation in both countries. In Chapter 8 we already noted the unusually large number of leading US high-tech and cyber firms active in Israel, as well as the outsized presence of Israelis in the US high-tech sector. The willingness of private US investors to fund Israeli startups has greatly eased their access to the US high-tech hubs, which is of course key to further success in the world market.[30] Israeli cyber firms provide thousands of jobs and billions of dollars in revenue in Massachusetts alone.[31] The US Chamber of Commerce hosts a US-Israeli Cyber Security Task Force designed to formulate joint cyber security policy, strengthen bilateral cooperation and innovation, and promote legislation fostering cyber security and information sharing.[32]

The Technion, Israel's equivalent of MIT, established a joint campus with Cornell in New York City, which deals with cyber security and a variety of other high-tech areas.[33] The campus is part of a broader $100 million initiative by the city of New York designed to turn it into an International Cyber Center, a global leader of cyber security innovation and a hub for startups. SOS, the Tel Aviv startup network, was chosen to establish the center, while Jerusalem Venture Partners, a leading Israeli venture-capital firm, was selected to lead the investment and innovation hub.[34]

China—lured by its vast market, Israel assigns top priority to expanding commercial ties with China. China, for its part, is interested in gaining access to innovative technologies and has built a strategic presence in Israel through a growing investment portfolio of high-tech startups, sensitive technologies, and infrastructure projects.

China has become a leading player in Israel's cyber industry. It ranks a close second to the US in the number of high-tech projects that it has cosponsored with Israel's Innovation Authority and accounted in recent years for one third of all investments in Israel's high-tech sector. Overall, China has become Israel's third largest trading partner, after the EU (as a bloc) and the US. Bilateral trade

between Israel and China grew 200-fold between 1992, when relations were first established, and 2017.[35] In recent years, however, the rate of growth has decreased.

The US has expressed growing concern over Chinese investments in Israel, citing security considerations and warning that it might be forced to limit intelligence sharing with Israel and possibly even security assistance as a result. US concerns have focused on three primary factors: market penetration and investment in Israel by leading Chinese firms, including Huawei and ZTE, two of China's biggest network equipment makers, which the US regards as potential espionage threats, especially in the emerging 5G cellular area; Israeli-Chinese cooperation in sensitive and early-stage technologies, including cyber; and Chinese investment in major Israeli infrastructure projects, including ports and rail projects.[36]

Under US pressure, and the conflicting strictures within the strategic culture to both maintain a major power patron and independence of action, Israel ceased weapons sales to China in the early 2000s. A gray area continued to exist, however, regarding dual use technologies, including cyber security and AI products, which can be used for espionage, surveillance, and intelligence purposes.[37] In practice, Israel had already taken some measures, of its own accord, to address concerns such as those raised by the US. Most Israeli defense companies recommend against or even forbid their employees from buying Chinese made cell phones, and the IDF has barred senior officers from doing so. The IDF has also imposed restrictions on the procurement of computer equipment from China.[38]

Under ongoing pressure, Israel also acceded to a US demand that it establish an oversight mechanism for foreign investment in its high-tech and infrastructure firms, directed primarily at China. In the attempt to minimize the blow to its economic ties with China, Israel tried to slow implementation of the oversight mechanism and compliance has remained voluntary. In 2020 Israel joined over 40 countries in adhering to the US "Clean Network Initiative" and was further poised to sign a bilateral MoU with the US regarding the safety of 5G networks. Both measures were designed to further minimize China's role in Israel's communications market and ensure the security of its communication systems. In 2022 Israel effectively barred Chinese firms from participating in a major rail infrastructure project, part of the new Tel Aviv Metro.[39]

How to address ongoing US displeasure over its ties with China, while at the same time trying to minimize the blow to the heretofore burgeoning commercial relationship with China, will continue to pose a major challenge for Israeli decision makers in the years to come. At the time of this writing, there has already been a three-year-long decline in Israeli-Chinese investments and trade.[40]

United Kingdom—the British cyber system draws significantly on Israel's experiences and is at least partially based on the Israeli model.[41] Cyber

cooperation with the UK has grown considerably, especially since 2014, when the two countries signed an MoU on Bilateral Digital Cooperation. This provided for collaboration in three primary areas: an exchange of information and experience regarding "open markets, open standards and open sources," digital public services, and cyber issues at the international level.[42] In 2021 a 10-year MoU and "strategic plan," covering defense cooperation in a variety of areas including cyber security, was signed. Israel was officially named a "tier 1" cyber partner of the UK, with greater access to its market. Among the provisions is a pledge to forge a closer alliance on cyber and tech, to "help to ensure that future standards on new technology are shaped by democratic nations."[43]

Israel and the UK are also reportedly engaged in extensive intelligence cooperation, including in the area of cyber security, and both countries' CERTs share information on cyber attacks. The response to the North Korean WannaCry attack, which severely disrupted the British health system, was an early example of this cooperation.[44]

In 2015 the UK Security and Information Agency and Israel's Ministry of Science, Technology and Space, together with the INCD, established a joint fund to promote cyber R&D between Bar Ilan and Haifa universities and the University of Bristol, University College London, and University of Kent. Identity management, cyber governance, privacy assurance, mobile security, and cryptography are among the areas of particular focus. Later that year, further agreement was reached on expanded cyber cooperation, including improved cyber education in schools and training exercises to strengthen cyber preparedness.[45]

Israel and the UK, together with South Korea, Estonia, and New Zealand, were the founding members of the "Digital 5 Group of Leading Digital Governments," an informal grouping of states with prominent records in digital government. Canada, Denmark, Portugal, Uruguay, and Mexico joined in subsequent years, making it a Group of 10. Established in 2014, the group aims to promote best practices in the cyber realm, innovation, an open digital economy, and open Internet.[46]

Between 2011 and 2018 the UK-Israel Tech Hub led to innovation partnerships worth £800 million to the British economy alone, much of this in the area of cyber security, the hub's flagship innovation exchange program. The Tech Hub has also led to a variety of other areas of cooperation and seeks to encourage British companies to establish R&D facilities in Israel. Two that have done so, the Royal Bank of Scotland (RBS) and HSBC, built permanent innovation centers.[47]

India—in 2017 India and Israel publicly agreed to deepen cyber security cooperation, but provided no details as to what that meant. The Indian Department of Science and Technology and Israel's Ministry of Science, Technology and

Space also signed an MoU providing for joint research in the areas of cyber security and big data analytics in healthcare. In 2018 a formal agreement providing for enhanced bilateral cooperation was concluded. The agreement included, inter alia, human resources development, enhanced cyber security resilience, and measures designed to make it easier to establish business-to-business ties.[48]

In 2019 an Israeli delegation headed by the INCD visited India and held a workshop and bilateral meeting with India's CERT. Twelve Israeli cyber firms took part in the delegation and met with representatives of 70 Indian cyber firms, presenting solutions for the finance sector and critical infrastructure. The Israel Export Institute also held its fifth professional seminar in India that year, CYBER EDGE, designed for national level decision makers and leaders in the critical infrastructure sector.[49]

In 2020 a further cyber agreement was signed, providing for the establishment of a framework for more regular bilateral dialogue, enhanced "in-depth operational cooperation," expanded exchanges of information on cyber threats, cooperation in capacity building, and mutual exchanges of best practices. As part of the agreement, the two countries' CERTs also signed a separate MoU.[50]

Japan—Israel and Japan signed a cyber security MoU in 2017 providing for increased investment, joint training programs, and contributions by Israeli experts to a new cyber security center of excellence in Japan.[51] A coordinating body was also established to promote collaborative work in artificial intelligence, robotics, the IoT, and autonomous driving.[52] In 2018 a further MoU expanded the areas of cooperation to cyber security R&D, information exchanges, and additional training programs.[53] In 2022 an MoU was signed between the two defense establishments which included cyber defense.[54]

A wave of ransomware attacks in Japan in 2018 led to an agreement regarding Israeli assistance in protecting Japan's cyber networks in preparation for the 2020 Olympics in Tokyo.[55] A shared concern over North Korean nuclear proliferation and Chinese cyber warfare capabilities has reportedly also led to growing cooperation on both the commercial and military levels.[56] NEC, a Japanese firm, established an R&D center in Israel dealing, inter alia, with cyber.[57] In 2021 the Fujitsu Cyber Security Center of Excellence was established in Beersheba, in partnership with Ben-Gurion University. The new cyber security center focuses on joint R&D to develop security technologies for AI-based systems.[58] By 2021 Japanese investment in Israel's tech sector accounted for 15% of all foreign investment, approximately tripling between 2019 and 2021 alone.[59]

Australia—Israel and Australia have conducted bilateral discussions on their respective cyber strategies, methods of building national cyber capacity and ecosystems, international law and norms in the cyber realm, and the IoT. A shared threat perception from Islamic extremism, in Australia's case primarily from ISIS in the Philippines, has contributed to heightened defense cooperation,

including cyber security.[60] In 2017 the bilateral dialogue was upgraded, with the signing of a new defense MoU. Both sides stressed the importance of cyber capabilities to ensure the resilience of their national security systems, while also stressing their intention to promote expanded commercial ties.[61] Israel's Ministry of Economics signed an R&D agreement with the Commonwealth Bank of Australia that included cyber security.[62] A joint industrial R&D agreement was signed between the Australian state of New South Wales and Israel, including funding for joint research in the field of cyber security.[63]

Germany—cooperation between Israel and Germany, Israel's third largest trading partner, is quite limited in the cyber realm. In 2011 the two countries signed a Joint Declaration of Intent on cooperation in cyber security, cyber crime, and joint R&D. German firms have demonstrated interest in Israel's innovative cyber security capabilities, especially in the area of autonomous vehicles. Fraunhofer SIT, among Europe's most important cyber security firms, established a Cybersecurity Innovation Center in Israel, which focuses on bridging the innovation gap and accelerating development of secure software, systems, and services. Deutsche Telekom, which opened offices in the Cyber Spark Advanced Technology Park adjacent to Ben-Gurion University, further expanded its collaborative efforts with the university, with a focus on network security, big data, and machine learning.[64]

In 2017 the German Cyber Security Council, a joint forum of business and political leaders, opened its first international chapter anywhere in Israel. It also signed an MoU with Israel Advanced Technology Industry (IATI), an umbrella organization of Israeli high-tech firms, designed to further promote bilateral cooperation in areas such as the Internet, cloud and critical infrastructure security, and privacy.[65]

Canada—the 2014 Canada-Israel Strategic Partnership provides for an exchange of information on the two states' national cyber security policies and best practices, as well as cooperation between the two CERTs.[66] Shared concerns regarding the threats to critical infrastructure led Israeli and Canadian energy firms to establish cooperative cyber security efforts, while the threat to the financial sector has similarly affected banks in both countries.[67]

UAE and Bahrain—the critical role that "cyber diplomacy" has played in Israel's foreign relations was illustrated by the dramatic normalization of relations with the United Arab Emirates (UAE) and Bahrain in 2020. Indeed, further expansion of long-standing but unofficial cyber cooperation, part of a shared perception of threat from Iran, was one of their primary motivations for developing ties with Israel, as was enhanced access to commercial Israeli cyber technology. One of the first bilateral meetings to take place following the diplomatic breakthrough was a meeting between the head of the INCD and his UAE counterpart.[68]

Formal bilateral cyber cooperation agreements, such as Israel has signed with numerous states, have apparently yet to be signed with either the UAE or Bahrain. Cyber cooperation has expanded, nevertheless, primarily with the UAE, with which dozens of meetings have taken place by senior Israeli cyber officials.[69] An agreement was concluded regarding cyber security in the healthcare arena. In 2021 the "UAE-IL tech zone" was launched by private businesses and the UAE hosted an Israeli cyber exhibition; both initiatives were designed to build connections between the two states' technology industries. The UAE also established an investment fund focused on cyber and other emerging technologies that reportedly is to spend $10 billion on Israeli firms.[70]

The UAE and Israel appear to be sharing intelligence regarding cyber threats, including an attack by Hezbollah that targeted both states. Discussions are also underway regarding the possibility of holding joint cyber defense exercises. Israel's state-owned Rafael Advanced Defense Systems and the UAE's Group 42 established a cyber R&D center in Israel. With the backing of the INCD, Rafael also announced the establishment of a consortium of Israeli firms, based in Dubai, to provide cyber security solutions for operating technology (OT) systems of particular interest to the UAE, such as power and desalination plants, seaports, and more. More controversially, the UAE has purchased offensive cyber tools from a number of Israeli firms, including NSO (see Chapter 8). Another firm, UAE-based DarkMatter, which has been accused of being a spy organization for the government, has heavily recruited veterans of Unit 8200, offering highly attractive incentives.[71]

Overall ties with Bahrain have also improved following normalization, though more slowly than with the UAE. The main appeal for both sides appears to be Israeli access to Bahrain's cyber security market. While smaller than the UAE's, it will likely gain a meaningful boost from ties to Israel.[72]

Morocco—in 2021, less than a year after the Abraham Accords were concluded, Israel and Morocco signed a cyber defense agreement "for operational cooperation, research and development and the sharing of information and knowledge."[73] Following the agreement, Israeli and Moroccan cyber security teams have been cooperating regarding defensive cyber operations, including an exchange of information about cyber threats and hacking attempts.[74] Israel's goal is to create real-time working teams and shared cloud-based tools, which will require building a high level of trust over time.[75]

Singapore—recent years have seen a marked growth in bilateral cyber cooperation, in both the commercial and governmental sectors, with Singapore. The two governments and various trade groups have held a number of events designed to further promote cyber cooperation, and numerous private firms work together in the cyber realm. Academic ties have also been growing, in areas such as emerging threats, new technologies, smart cities, and the IoT.[76]

Israel and Singapore reportedly share intelligence information regarding cyber threats and work closely together regarding cyber defense. Illustrating this point, state-owned Israel Aerospace Industries has numerous ties to Singapore, including a major R&D cyber early warning center and a part in a government project designed to develop new technologies regarding digital crime.[77]

Cyber cooperation with other states—Israel's very first bilateral cyber agreement was signed with **Italy**, in 2013.[78] In 2018, as part of Israel's emerging trilateral alliance with **Greece** and **Cyprus**, a cyber security cooperation agreement was signed, providing for information sharing and operational cooperation. The rapid development of Greece's defense industries in recent years, including in the cyber area, may provide the basis for expanded cooperation.[79] In 2019 the INCD helped **Romania** counter a massive ransomware attack against hospitals and a bilateral cyber security R&D agreement was signed in 2020.[80] In 2020 the INCD helped the **Czech Republic** counter a large scale cyber attack on hospitals and academic research centers dealing with the coronavirus[81] and the Czechs appointed a cyber attaché to their embassy in Israel.[82] In 2020 a cooperation agreement was signed with **Kazakhstan.** That same year the head of the INCD made a special appeal to **African** nations to strengthen their cyber cooperation with Israel, and a cooperation agreement was signed with **Congo**.[83]

Multilateral cyber cooperation—in 2016 the INCD and **World Bank** jointly hosted a capacity building workshop in Israel, designed to share expertise in the areas of cyber security policy, strategy, and technology of a best practice country. The workshop focused on Israel's experience in the establishment of national cyber institutions, identification and protection of critical infrastructure, cyber crime, and more. Participants also met with the heads of the INCD, CERT-IL, incubators, start-ups and established firms, academic experts, and officials involved in securing the electric grid.[84] In 2019 Israel signed an agreement with the World Bank's Digital Development Partnership to promote cyber security in developing nations in Africa, Latin America, and Eastern Europe. In partnership with the UK, Japan, Finland, Denmark, Norway, and others, Israel was to share its expertise regarding protection of critical infrastructure.[85]

Israel has also signed cooperation agreements to promote cyber security in developing nations with the **Inter-American Bank for Development**, with which it has already held a two-week training workshop for cyber professionals from 22 Latin American countries, and the **World Economic Forum**. In 2020 the INCD launched an international platform for sharing real-time Covid related information. That same year Israel's premier annual cyber security conference and exhibition, CyberTech, jointly sponsored by the INCD and other entities, attracted 18,000 participants from Israel and around the world, including representatives of 200 different companies. In 2021 Israel hosted the annual **Organization of Economic Cooperation and Development** (OECD) conference regarding the

cyber realm, which ended with a pledge by the participating states to continue to build connections and enhance cyber cooperation.[86]

In 2021 Israel led a 10-day-long simulation of a major cyber attack on the world's financial system, with the participation of 10 countries, including the US, UK, UAE, Germany, Italy, and Switzerland, as well as the IMF and World Bank. The simulation included several types of attacks that impacted global foreign-exchange and bond markets, liquidity, integrity of data, and transactions between importers and exporters.[87]

In 2018 the IDF hosted its first international digital and cyber conference, with 70 representatives from 11 countries, including the US, UK, South Korea, Austria, Canada, the Netherlands, Italy, Rwanda, Japan, Hungary, and Poland. In 2019 the IDF also opened its doors to foreign military delegations interested in training at its advanced cyber simulator.[88]

Thought was given in the past to the establishment of an international cyber development assistance agency, to complement the Foreign Ministry's already existing Mashav general international assistance department. Unsurprisingly, both the Foreign Ministry and Treasury were opposed, the former for reasons of bureaucratic turf and the latter for budgetary reasons. The INCD itself did not have the budget to finance the new agency on its own and was preoccupied, in any event, with its own organizational development processes. Bureaucratic competition similarly stymied the appointment of a national "cyber ambassador," as opposed to the current situation, whereby the Foreign Ministry has a lower level official responsible for cyber affairs and the INCD has a department responsible for international cooperation.[89]

International Cyber Norms, Agreements, and Law

International norms, agreements, and law can provide states with an additional array of tools with which to strengthen their cyber security, over and above their general importance for the moderation and regulation of an anarchic state system. Support for the application of international norms, agreements, and law in the cyber realm is based, as in other realms, on the assumption that malicious actors will fear adverse consequences and be increasingly constrained in their behavior to the extent that they believe that they are likely to confront a coalition of states. The larger the coalition of states supporting the international norms, the greater the consequences the violator will likely suffer, although in some cases a smaller but more coherent coalition may be able to present an even stauncher and more effective common position.[90]

Leading cyber actors, including the US, UK, Russia, and China, have all expressed interest in the development of international cyber norms and law

and have taken part in various efforts to establish them, as have major international corporations.[91] A variety of international groupings and organizations have also called for the adoption of international norms and law in the cyber realm. Some of the more prominent among them include the EU, NATO, OSCE (Organization for Security and Cooperation in Europe), ASEAN, Shanghai Cooperation Organization, African Union, and the G-20.[92] Leading standards organizations and various public groups, such as Human Rights Watch, have also pushed for the creation of international cyber norms.[93]

It is important to note that not all actors mean the same thing when they refer to international norms. The UN Group of Governmental Experts (UNGGE) (elaborated on later) refers to "voluntary, non-binding" norms that do not replace international law, but rather seek to buttress it and set standards for responsible state behavior. Major multinational corporations such as Microsoft have called upon states to make binding commitments and refrain from misusing their networks. Russia, China, and others support norms that supplant existing international law.

At present there are only two relatively widely accepted and adopted international agreements in the cyber realm, the 2001 Budapest Convention on Cybercrime (including an Additional Protocol from 2006) and the 2009 Shanghai Cooperation Organization's International Information Security Agreement. The Budapest Convention has led to heightened cooperation between law enforcement agencies in 64 states, including Israel, but Russia and China, among others, have refused to join, thereby limiting its effectiveness as a global regime.[94] In 2017 Russia presented a detailed proposal to replace the Budapest Convention, but encountered strong opposition from the West, which was concerned that the Russian proposal would strengthen authoritarian states' control both over domestic and international communications. In 2019, over US opposition but with China's support, the General Assembly approved a Russian resolution to begin drafting a new convention.[95]

The disagreement surrounding the Russian proposal highlighted the fundamental differences between the approach of Western states toward the cyber realm and that of authoritarian states. Whereas Western states, including Israel, support a free and open global Internet, without national boundaries, and are deeply concerned about protection of civil liberties in the cyber realm, authoritarian states fear that these conditions may be used to undermine their regimes. Russia and China thus advocate a new Internet governance model that would provide for greater state control and sovereignty, rather than the "multistakeholder" balance between governments, the private sector, interest groups and individuals advocated by the West. To this end they have proposed that the International Telecommunications Union (ITU) and other UN-sponsored organizations, which they believe they can dominate, replace ICANN, the nonprofit

originally established by the US as the international Internet governance body. For Russia, which calls for resistance to "Western digital neocolonialism," China and other authoritarian states, cyber capabilities are a mere extension of already existing coercive instruments of power and a part of their broader national sovereignty, which provides them with the right to manage the Internet within their territory as they deem appropriate. In 2021 Russia and China concluded a new agreement incorporating this shared approach.[96]

The UNGGE was established in 2004 in one of the earliest attempts to address the applicability of international law to the cyber realm and has been the focus of UN efforts in this area ever since. Among other measures, the UNGGE has concluded that existing international law is applicable to the cyber realm and thus that states must meet their international obligations to refrain from "internationally wrongful acts," including the prohibition on the use of force, the requirement to respect territorial sovereignty, and the principle of peaceful resolution of disputes. It called on states to adopt voluntary, non-binding cyber norms, conduct enhanced inter-governmental exchanges of information on cyber threats, adopt measures to protect infrastructure from cyber attack, and protect cyber privacy and freedom of expression. The UNGGE further recommended that states ban cyber attacks from the territory of UN member states, especially against emergency response teams and critical infrastructure, as well as ban the use of proxies to conduct cyber attacks.

UNGGE meetings in 2017 and 2018 failed to yield significant further progress, largely due to tensions and disagreement between the US and other Western states. The 2021 meeting further refined 11 voluntary and nonbinding cyber norms originally recommended in 2015.[97] As an informal group of experts, rather than official representatives, the UNGGE's findings are non-binding.[98] Israel was invited to participate in the 2015 UNGGE meeting, but a combination of the conveners' desire to maintain the group's small size and, in all likelihood, diplomatic considerations stemming from Israel's international status, prevented it from being invited once again in subsequent years.

In 2013 and 2017 an International Group of Experts, working under the auspices of NATO, crafted the Tallinn Manuals. Probably the most ambitious attempts to date to address the applicability of international law to the cyber realm, most of the manuals' authors agreed that existing law is applicable, with some necessary modifications. The 2013 manual focused on international law as it applies to cases of "armed conflict" and "armed attack," which may trigger a nation's "right to self-defense" under the UN Charter and, subject to various limitations, consequent decision to respond with force. The 2017 version looked at a broader spectrum of activities in the cyber realm, those that actually make up most cyber incidents but fall short of the threshold that triggers the right to self-defense.

Crucially, the crafters of the Tallinn Manuals were unable to reach agreement on a number of key issues, including the precise conditions for treating a cyber attack as an armed attack, whether cyber attacks that do not cause significant injury, death, physical damage, or destruction constitute armed attacks, or the threshold that triggers a state's right to self-defense. Cyber attacks that do cause these effects were deemed to be the equivalent of an armed attack and international law in the cyber realm was held to apply to nonstate actors, such as terrorist groups, as well as to state actors. The principle of "distinction" between civilian and non-civilian targets that exists in the physical world was also deemed to apply to the cyber realm. GPS or air traffic control systems, for example, that can serve both civilian and military purposes, thus qualify as legitimate military targets, as do persons directly involved in cyber hostilities. The principle of distinction, however, still applies and prohibits indiscriminate cyber attacks on civilian targets, for example, a computer virus that spreads and destroys civilian systems uncontrollably or one that is introduced into a military system but spreads randomly into civilian systems.

The Tallinn Manuals, at least according to their authors, did not propose new international law in the cyber realm, rather an effort to offer an interpretation of the applicability of existing ones. Others, including the US, UK, Germany, and Israel, question whether this was indeed the case, and a consensus has yet to emerge regarding some of the conclusions even among the states that sponsored the manuals. In any event, their recommendations, much like those of the UNGGE, are not binding but constitute an important discussion among experts designed to advance legal understanding of the issues considered[99] and are likely to guide many states' behavior as the debate unfolds.

In 2018 Russia formed a new UN group, under its leadership, called the Open-Ended Working Group (OEWG). Participation is open to all UN member states, unlike the small group involved in crafting the UNGGE, and Israel, too, has participated. In 2021 the OEWG issued a report stating that voluntary, nonbinding norms of responsible state behavior in the cyber realm can contribute to the prevention of conflict and reflect the expectations and standards of the international community. There was also general agreement regarding the importance of confidence building measures as a means of preventing conflict. Beyond that, the differences in approach were stark.

China and others were of the opinion that international norms and principles are binding and take precedence over existing international law. They were also opposed to the applicability of the UN Charter and international law to the cyber realm, arguing that this would legitimize its militarization and increase the likelihood of resort to conflict in any domain. The US, EU, and others took the opposite view, that international norms are non-binding and that existing international law is applicable to the cyber realm. Further, disputes revolved around

the applicability of specific principles of the UN Charter to the cyber realm, such as state sovereignty and nonintervention in the affairs of other states, the right to invoke self-defense, distinction, proportionality, and necessity. The need for resolution of disputes by peaceful means was an outlier as it was the one area of agreement.[100]

Some believe that Russia seeks to use the OEWG to supplant the UNGGE, potentially politicizing what had heretofore been a professional discussion of complex technical issues.[101] The US, EU, Japan, and other states thus seek to replace the dual track of the UNGGE and OEWG with a single and permanent UN forum. Russia, China, and others, however, seek to keep the OEWG framework.[102]

France has expressed support for a "new path" in the cyber realm, different both from the "Californian form of Internet," in which the government allows private firms to make decisions with far reaching socioeconomic implications, and the "Chinese Internet," in which the government drives innovation and controls the cyber realm.[103] In 2018 France proposed the "Paris Call for Trust and Security in Cyberspace," designed to promote international cyber norms, including prevention of interference in elections, hacking back, attacks on the public core of the Internet, attacks on critical infrastructure, and intellectual theft. More than 75 states have endorsed the plan, including the EU, UK, Japan, Canada, New Zealand, and South Korea, as have Microsoft, Facebook, Google, IBM, and HP. Conversely, a highly unusual grouping of the US, Australia, Russia, China, North Korea, Iran, Israel, and other states—some of the most active cyber actors—have not, nor have Amazon and Apple. The comparatively broad support from private sector entities distinguished the "Paris Call" from other attempts to promote cyber norms and reflected the leading role now played by the primary multinational corporations. Microsoft, which has proposed a Cyber Security Tech Accord of its own, signed by more than 60 technology corporations,[104] stands out in particular for its support of this effort.

In 2019 the Global Commission on the Stability of Cyberspace, a group of experts from government, industry, and civil society, proposed a set of eight norms designed to regulate behavior in the cyber realm. They included: noninterference in the availability or integrity of the Internet, electoral systems, and product development processes; a prohibition on taking control of private computers to create botnets; a process to enable disclosure and repair of vulnerabilities in software and hardware; securing cyber infrastructure, including software and hardware; promotion of cyber hygiene; and preventing nonstate actors from using the cyber realm to launch attacks. These, however, are non-binding recommendations.

Considerable controversy remains over the applicability of international humanitarian law and the Law of Armed Conflict (LOAC) to the cyber realm,

despite general agreement that many of the principles do apply. Much of the debate revolves around some of the same issues considered by the Tallinn Manuals, especially the differing interpretations of what, under the UN Charter, constitutes a use of force, or armed attack, in the cyber realm and a state's consequent right, in the latter case, to act in self-defense. Under the LOAC intentionally targeting civilians is forbidden, as is a failure to take appropriate measures to limit collateral damage, and attackers are enjoined to ensure that they cause as little damage to civilian populations and infrastructure as possible.[105]

The US and Western states continue to take the position that existing international law, including the LOAC, apply to the cyber realm as is, whereas Russia, China, and others have taken a more equivocal stance. Broad agreement does exist around the principle that the nature of the target and of the harm caused, whether physical damage or death, are the critical factors that determine whether an attack constitutes a use of force or armed attack, much as in the case of traditional military means such as missiles or mines. Differences persist, however, regarding the threshold that triggers the right to self-defense. The US and others have sought to broaden the definition of the attacks covered, to include, for example, cyber attacks on critical infrastructure that do not result in physical destruction or death and attacks with severe financial ramifications.[106]

Of late, a growing number of states (e.g., Australia, Finland, Netherlands, New Zealand) do seem to at least implicitly support this broader approach and take the "scale and effects" of the cyber attack into account, as suggested by the Tallinn Manual. France has taken the clearest position, stating unequivocally that a cyber attack need be neither destructive nor injurious to violate the prohibition on the use of force and that it would consider a cyber attack on its economy the equivalent of an armed attack, thereby triggering the right of self-defense.[107] The very act of figuring out what damage had been caused by a cyber attack further complicates this calculation. Cyber weapons can cause damage that cannot be readily discovered, and they also have unintended consequences.[108]

Dual-use technologies, those with both civilian and military applications, pose a further difficulty. Military and civilian networks often overlap and cyber attacks against one can also cause damage to the other. It is thus difficult to determine whether civilian or military targets have been attacked and whether the LOAC should be applied. Social media networks, such as Facebook and Twitter, are used as channels for communicating information of a military nature, or even as part of actual cyber operations, further complicating matters. The speed of digital innovation further complicates efforts to develop international cyber law generally.[109]

Outside of situations of armed conflict, international law only applies to states and international organizations, not to commercial entities such as the giant multinational firms that wield outsized power in the cyber realm today. These

firms build and run the global cyber architecture, largely govern the flow of data, and provide critical civilian and military services to governments, without which they cannot carry out their functions. Furthermore, unlike most international law, many cyber norms today are adopted, in practice, in the commercial agreements made by the multinational firms, but these firms are accountable, if at all, only to their shareholders.[110]

A further obstacle to the formulation of effective international cyber norms and law is a concern that some states, for example, China, might derive economic gain from a theft of intellectual property that would outweigh any penalties imposed, rendering them ineffective. Abuses of the cyber realm to curtail freedom of political expression constitute another major source of concern.[111] With certain limited exceptions, there is general consensus that cyber espionage alone, in which no physical harm or loss of functionality is caused, does not constitute a violation of international law. The SolarWinds attack in 2020, for example, one of the most dramatic cyber attacks ever (see Chapter 2), in which Russia breached tens of critical Western targets for intelligence purposes but did not cause physical harm or loss of functionality, would thus not constitute a use of force or trigger an armed conflict.[112] Some legal experts maintain that the Stuxnet attack, in contrast, the alleged US-Israeli cyber attack that caused physical damage to Iran's nuclear centrifuges (Chapter 10), did constitute an illegal use of force and thus a violation of international law but that the damage caused was insufficient to amount to an armed attack and thereby trigger Iran's right to self-defense.[113]

In recent years, growing international agreement appears to be emerging regarding another contentious issue, whether states are responsible for cyber attacks perpetrated by nonstate actors operating out of their territory. The emerging agreement holds that they are responsible, but only if the state in question provided actual support, not merely sanctuary.[114]

Some go beyond the adoption of international norms and existing law and advocate an international treaty specifically designed to regulate cyber warfare. As with earlier arms control agreements, proponents hope that a treaty of this sort will help promote deterrence and greater international stability. To be truly effective, a cyber treaty such as this would require the participation of a large number of states and have to establish rules that effectively govern state behavior, reduce uncertainty through credible information sharing procedures, provide an effective monitoring mechanism, and impose significant costs for failure to comply. Conversely, the more binding an agreement, the more reluctant states may be to join and allow restrictions on their behavior.[115] At this time, the prospects for a cyber treaty of this nature appear far off.

A particular concern regarding the viability of a cyber treaty has to do with the issue of verification, a fundamental pillar of traditional arms control agreements,

whether for conventional or unconventional weapons. In the cyber realm it is very hard to distinguish between offensive weapons and those designed for counter-attack or defense, in fact, the entire difference may be no more than a few lines of computer code. To a far greater degree than in the physical world, it is also fairly simple to destroy evidence of an attack before inspectors can arrive.[116] Adding to this, the US and others are concerned that Russia, for example, would simply deny responsibility for cyber attacks conducted by nonstate actors operating at its behest and falsely claim to be in compliance with the agreement. All of this is further complicated by the great lengths that states go to hide their cyber weapons. When states cannot be held accountable for their actions, norms and treaties cannot constrain their behavior.[117]

Further contributing to the difficulties of verification, many of those who conduct cyber attacks are neither members of nor subordinate to national militaries or governments. When compared to existing arms control agreements, the range of potential actors that would have to be covered by a cyber treaty is far broader: not just states, but nonstate actors, such as state-affiliated proxies, terrorist organizations, private firms, and various public groups, even individuals, who would undoubtedly be strongly opposed to inspections of their facilities or personal devices. These nonstate actors also expand the ways in which states can avoid detection when they choose to violate the agreement.[118]

Finally, and as was the case in regard to arms control agreements in the past, advanced cyber powers would be concerned that lesser adversaries might seek to make use of a cyber treaty (and international norms, agreements, and law generally) to curb their advantages and close the technological gap without truly limiting their own activities. These powers would thus likely be loath to support the adoption of such arrangements, especially in regard to offensive capabilities.[119]

Israel and Cyber Norms, Agreements, and Law

In 2020 Israel gave the most detailed and authoritative presentation to date of its positions regarding international law and the cyber realm.[120] The presentation was the product of a multi-year inter-agency process,[121] thereby demonstrating the importance attached to it.

Israel believes that international law is applicable to the cyber realm, but appropriate caution must be exercised when applying existing legal rules to different technological domains in which accepted practices regarding seemingly similar activities may not truly be similar. To illustrate, whereas ground forces may not transit another state's territory without its express consent, naval vessels and aircraft may cross its territorial waters and airspace freely, subject only to certain limitations. Code and data, however, are routed through other states'

networks automatically, as a matter of course. Moreover, technological change in the cyber realm is very rapid, further warranting an approach of due legal caution. Israel thus reaffirms the general applicability of international law to the cyber realm, but not necessarily particular rules. This overall cautious approach toward the applicability of international law to the cyber realm and the need to test its practical ramifications over time had been typical of Israel's positions as early as the discussions in the UNGGE during 2013–2015.[122]

Israel further takes the position that when a cyber attack, much like a kinetic attack, can reasonably be expected to cause death or injury to persons, or physical damage to objects, for example, when hacking a railroad network is likely to cause a collision, it amounts to a use of force and is thus forbidden under international law. A cyber attack might also constitute a use of force and be forbidden if a loss of functionality was the secondary effect of the physical damage that it had caused, for example, if an aircraft crashed as a result of a cyber attack that shut down electricity in a military airfield. Similarly, Israel holds that a cyber attack involving the deletion or alteration of data would constitute an attack under the LOAC if it could be reasonably expected to cause physical harm to persons or objects. More controversially, Israel does not consider a mere loss or impairment of functionality to infrastructure to be a use of force, much as certain types of electronic and psychological warfare or economic sanctions are not.

Much like most other states, Israel has not specified the threshold that determines whether a cyber attack with non-physical effects, such as on a state's economy, constitutes a use of force or armed attack. It has also yet to indicate whether the thresholds for the two are distinct, or identical as the US believes. A number of states have adopted the "scale and effects approach" mentioned earlier but have not provided any specifics, beyond suggesting that they should be comparable to those that would qualify a non-cyber operation as a use of force or armed attack.

Israel has long been of the position that the right to self-defense applies to attacks conducted by nonstate actors, not just state actors, and believes that this general position applies to cyber attacks as well. This approach is shared by the US, UK, and Netherlands, but is disputed by others, such as France. Israel further believes that a state under cyber attack, either by a state or nonstate actor, may act in accordance with the right to self-defense, when the use of force constitutes an actual or imminent armed attack, subject of course to the customary principles of necessity and proportionality. The fact that a cyber operation may not constitute an armed attack does not, however, mean that no legal limitations apply. Israel believes that there are general obligations under the LOAC that apply to all military operations, whether they constitute an armed attack or not, first and foremost, the requirement to consider the danger to civilian populations.

Israel further believes that only tangible things can constitute "objects" for purposes of international law. This approach is supported by most of the experts who drafted the second Tallinn Manual, but most states have avoided enunciating it openly to date.

Israel has yet to adopt a definitive position regarding the applicability of the principal of "sovereignty" to international law in the cyber realm, a violation of which would constitute an "internationally wrongful act." States may have legitimate interests regarding data that is not located in their sovereign territory, for example, when stored on cloud services provided by third parties abroad. Further muddying the picture, states legitimately conduct cyber activities that transit foreign states and may even target networks and computers in other states for purposes of national defense, cyber security, or law enforcement, and it is unclear under existing international law whether actions such as these constitute a violation of state sovereignty. Conversely, Israel believes that cyber operations that interfere with another state's internal or external affairs, for example, its ability to hold an election or that manipulate the outcome of the election, would constitute a clear violation of its sovereignty and thus be a wrongful act. So, too, would providing a nonstate actor with the technology, funding, or training necessary to conduct hostile cyber operations against another state actor.

In pursuit of the right to self-defense, Israel holds that a state may respond to a cyber attack with either cyber or kinetic means, much as it may similarly respond to a kinetic attack in the same way. This approach was manifested in practice in Israel's bombings of the Hamas cyber headquarters in 2019 and other cyber capabilities in 2021. Israel, like the US, UK, and others, further believes that a state is not required to provide another state with notification prior to conducting a cyber operation taken in response to a cyber attack against it. Events in the cyber realm occur extremely rapidly, and prior disclosure might render a countermeasure ineffective.

Israel further believes that a rule of due diligence, which would require states to take feasible measures to end hostile cyber operations affecting the legal rights of other states, has yet to emerge in the cyber realm, unlike other domains. One informed observer found this position surprising for three reasons: Israel presumably already acts to end cyber attacks such as these and would thus not be taking on an additional burden; a rule of due diligence would enable Israel to demand that other states take remedial action when it was the target of a cyber attack, as it frequently is; and it would open the door to Israeli countermeasures against states that fail to comply with the requirement, whether by pressuring them into compliance or directly putting an end to the hostile operation itself.[123]

Finally, Israel advises against attempts to over-regulate the attribution issue. Attribution capabilities are improving continually, even states with lesser capabilities are increasingly able to rely on information provided by other states

and the private sector, and consequently the need for greater legal certainty prior to attribution is becoming increasingly theoretical. In any event, Israel holds that the choice whether or not to disclose the information used to attribute an attack should remain at the state's exclusive discretion.

Concluding Observations—Israel, Cyber Cooperation, and International Law

Israel has turned its cyber capabilities into the basis for a new and successful form of "cyber diplomacy": that is, an important component of its national security thinking and the array of foreign and defense policy tools available to it. With the US, unsurprisingly, cyber cooperation is extensive in all areas, civil and military, with China civil cooperation is extensive, but in jeopardy, both due to US pressures to curtail it and Israel's own interests. With a variety of other countries, the UAE and other Gulf states in particular, cyber cooperation played a role in their decisions to establish relations with Israel, and various levels of cooperation exist.

The limitations of the publicly available information regarding the substance of Israel's international cyber cooperation are such that we are limited to just a few observations. First, there is broad recognition, throughout Israel's government, of the importance of international cyber cooperation and of participation in the international cyber dialogue, as instruments of diplomacy. This recognition, an outgrowth of Israel's strategic culture, has been manifested by the important role attached to international cooperation in every cabinet decision. Nevertheless, the effort does not enjoy sufficient central direction or funding, even personnel,[124] all of which would increase its efficacy.

Even Israel's participation in various multilateral forums, a comparatively inexpensive contribution to the international cyber dialogue, is modest. This is compounded by the INCD's puzzling failure to translate the numerous policy statements and directives it issues into English and other languages or to provide a description of the areas of cooperation it is interested in engaging in and the assistance it could provide. As a consequence, some potential partners are unaware of the practical benefits of cooperation with Israel, and the general public also remains unapprised of Israel's constructive contribution to international cyber security and to the international dialogue around critical cyber issues.

For Israel, which faces constant diplomatic pressure, this is an unfortunate waste of an opportunity. As a world leader in the cyber realm, there is considerable interest in hearing about and learning from Israel's experience and policies. The 2020 presentation, mentioned earlier, of Israel's positions

regarding international cyber law, was a notable exception to this failing. Part of the problem in presenting a coherent and unified national policy, especially in regard to international cyber law, is that Israel, like other states, is simply playing catch-up, trying to understand the intricacies of the rapidly changing technology and its legal ramifications. Part of the problem, however, is also a result of the difficulties in achieving inter-agency coordination and in formulating agreed policy in Israel's fractious political system. As a consequence, there is often a time lag between events and the enunciation of agreed policy.

The announcement by Prime Minister Bennett, in 2021, that Israel was inviting like-minded states to join in a global cyber defense shield, appears to be a recognition of its deficient involvement in multinational cyber cooperation. Whether the seemingly dramatic announcement was just rhetoric or a serious initiative remains to be seen. At the time of this writing, the answer appears to be the former.

The constant barrage of cyber attacks against Israel illustrates the particular difficulty that arises when seeking to apply international norms to the threats it faces. To date, most of these attacks have been conducted by nonstate actors, though they often have close ties to Iran. Even if it was possible to attribute the attacks directly to their source, at a level required by the international community, and if the level of damage caused was significant, not all states agree that Israel would be justified in invoking the right to self-defense.[125] Indeed, the pressure against such a counterattack might be significant, and Israel's ability to respond might be highly limited. Moreover, Israel, like other leading cyber powers, would presumably be quite hesitant to agree to limitations on the unique capabilities it has developed in this realm in the name of international norms of questionable effectiveness. The precision and long-range capabilities proffered by cyber weapons can be a particularly important instrument of warfare for a state such as Israel, which is typically pilloried in the international arena for causing collateral damage, whether or not it actually did.

Both former Prime Minister Netanyahu and the former head of the INCD Eviatar Matania have expressed support for the creation of *regional* cyber norms, along with skepticism regarding the feasibility of effective universal ones. Their hesitation apparently stems from a well-founded apprehension that the consensus required for universal norms will prove hard to achieve and that some states will violate them even if adopted.[126] Israel has bitter experience with regional actors that have repeatedly violated the international agreements they signed, including the Nonproliferation Treaty and Chemical Weapons Convention, and would be particularly concerned about verification issues, especially in regard to Iran.

In practice, profound differences in interests and approach continue to divide the primary cyber powers and make it doubtful whether effective and

enforceable international cyber norms can be achieved at any time in the foreseeable future.[127] Most of the norms that have emerged to date have been voluntary and non-binding, and a binding universal cyber agreement continues to prove elusive.[128] In Chapter 12 we recommend a number of cyber norms that Israel might be able to support, without jeopardizing its national security.

10

The Military Cyber Strategy

(Cyber) will soon be revealed to be the biggest revolution (in warfare), more than gunpowder and the utilization of air power in the past century.
Major General Aviv Kochavi, Head of Military Intelligence

(Cyber is) a playing field that we need to use to the fullest and I think that the State of Israel . . . must be at the level of a superpower.
Lieutenant General Benny Gantz, IDF Chief of Staff

In an anarchic self-help world, in which states must constantly strive to strengthen their national power, Israel has responded to the threats it faces by developing highly advanced offensive and defensive military capabilities. Self-help, or in the terminology more commonly used in Israeli strategic thinking, self-reliance, has also led to the development of highly advanced scientific capabilities and to a large and sophisticated domestic military industrial base.

Israel developed its cyber capabilities, first and foremost, in response to the emergence of a new and potentially severe military threat, as well as a military and economic opportunity. As such, and in accordance with realist international relations theory, Israel's cyber capabilities constituted a strategic imperative. They were, however, also a function of Israel's strategic culture. As suggested by constructivist thinking, this strategic culture affected how Israel defined its strategic circumstances and led to the choice of technological prowess as the basis for both its response to the threats it faced, including in the cyber realm, and the qualitative military edge with which it sought to offset its adversaries' advantages. As will be seen in this chapter, bureaucratic politics also played a significant role in the development of Israel's military cyber capabilities.

Chapter 10 adds the critical military dimension to our discussion of Israel's civil cyber strategy presented in Chapters 7–9. Chapter 10 has three main sections. We begin with what is publicly known regarding Israel's offensive and defensive military cyber strategy and raise the question of what part, if any, they might play in Israel's broader national security strategy, including its purported

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0011

nuclear capabilities. The second section provides a description of the primary IDF units involved in cyber operations, as well as those of the ISA and other relevant agencies. The chapter concludes with a detailed description of some of the primary offensive cyber attacks attributed to Israel to date, starting with Olympic Games and Stuxnet before turning to more recent attacks.

Offensive and Defensive Military Cyber Strategy

For the IDF, the cyber realm presents a new, fourth dimension of military operations, along with the existing dimensions of ground, sea, and air. It is also an area in which Israel enjoys unique advantages that stand to make an important contribution to the overall qualitative edge at the heart of its strategic culture. Unlike the public and private sectors, for which the INCD issued a formal cyber strategy based on readily available cabinet decisions, Israel's military cyber strategy, unsurprisingly, remains largely unknown and can only be partly surmised from a small number of public pronouncements, a few lines in the IDF Strategy, and observable behavior. Some believe that the IDF's cyber strategy is actually one of "cyber ambiguity," an analog of Israel's long-standing nuclear policy, in accordance with which it neither confirms nor denies the capabilities attributed to it but enjoys the deterrent benefits they provide, nonetheless.[1]

The IDF Strategy states, without further elaboration, that cyber operations will be conducted for defensive, offensive, intelligence, and information warfare purposes at all levels of conflict.[2] Various classified IDF documents address the cyber realm, including the threats and operational options it presents. Nevertheless, Israel has yet to formulate a comprehensive military cyber strategy or to integrate the military cyber realm into its overall national security strategy.[3] The Gideon Five-Year Plan for 2016–2020 was to have included the formulation of a written cyber operations doctrine at the General Staff level,[4] but this has apparently not happened.[5]

A Fundamentally Offensive Cyber Strategy —until the mid-2000s cyber was viewed by the IDF as a supporting element, a means of storing information and of assisting warfighting capabilities. Change happened rapidly, and by 2010 cyber had become integral to IDF warfighting capabilities, both in terms of the weapons used and the nature of warfare itself.[6] In 2009 the IDF formally defined cyber as a strategic and operational theater of operations and began allocating the necessary budgets and personnel.[7] Former Deputy Chief of Staff Yair Golan believes the IDF's cyber capabilities will eventually be so integrated into everything it does that they will cease to constitute a separate function and the IDF will no longer even be capable of conducting combat without them. Instead, cyber will be incorporated into every IDF formation down to the tactical level,

with a "cyber tank" in every company.[8] Nevertheless, the IDF views cyber as a complementary capability and not necessarily a decisive one.[9]

Cyber operations fit in well with the IDF's strategy of the campaign between the wars (MABAM) a series of its limited, ongoing, "below the radar" operations, designed to prevent enemy force build-up without provoking a major confrontation.[10] Crucially, cyber attacks alone are not considered sufficient to defeat an adversary, but may enable the IDF to strike important targets that cannot be reached by other means[11] and without having to risk soldiers' lives. Offensive cyber operations are also to be conducted to ensure the functional continuity of important state institutions.[12]

The fundamentally offensive nature of Israel's cyber strategy, in keeping with its long-standing strategic culture, was expressed in a series of public statements by senior defense officials. The head of the ISA, Nadav Argaman, stated that Israel does not make do with passive defense in the cyber realm, much as it does not in the physical world, and instead acts proactively to prevent cyber attacks by targeting hackers around the world. Argaman further stated that Israel's responses to cyber threats combine both cyber and kinetic measures and that the ISA and Mossad cooperate in cyber offense, at times together with foreign partners.[13]

A former head of the IDF Cyber Staff* similarly stated that Israel does not wait to be attacked and that the IDF's approach is one of active defense, in keeping with its long-standing preference for transferring the battle to the enemy.[14] Then Defense Minister Moshe Yaalon stressed that Israel would conduct cyber attacks not just in retaliation but for purposes of general deterrence.[15] The head of the INCD further strengthened the deterrent message by stressing that Israel has the "capability to respond forcefully to cyber attacks and not necessarily on the same vector as the attack."[16] For purposes of lower level attacks, retaliation is often inappropriate and even escalatory and runs counter to Israel's general cyber strategy, which is based on defense and deterrence by denial. For higher end attacks, deterrence by punishment becomes more appropriate.[17]

A series of public statements by former heads of Unit 8200 shed further light both on the importance and ambitiousness of Israel's offensive cyber thinking. One former head of the unit, Pinchas Buchris, stated that Israel's offensive cyber capabilities would enable it to counter the threat posed by Hezbollah's advanced rockets, although not the low-tech ones that comprise the bulk of its rocket arsenal.[18] Another former head of the unit, Yair Cohen, was even more expansive, stating that "it is not beyond imagination" that "with one keystroke, on the eve of a war, all enemy aircraft could be disabled without sending a single aircraft on a

* Now the Cyber Defense Brigade.

mission and without risking one human life."[19] Still another former head of Unit 8200, Ehud Schneorson, indicated that Israel can and should use cyber means to wreak havoc on Iran's energy sector at the start of a major conflict. A cyber attack such as this, he maintained, would have a broad strategic impact, whereas neutralizing Iran's weapons systems would only provide tactical superiority.[20]

The head of the IDF Planning Branch and later commander of the IAF, Major General Tomer Bar, stated that Israel's offensive operations would include kinetic, cyber, and electronic warfare attacks in the air, on the ground, and at sea. "Imagine," he stated, "that the enemy loses its ability to communicate prior to (an Israeli) aerial attack, its will to fight is undermined, its computers are shut down and it is then attacked with bombs . . . This is not imaginary, but things that the IDF has to do in a coordinated and synchronized manner."[21]

A study published in an open-source IDF journal in 2020 concluded that while IDF cyber operations have already had a significant impact on the regional balance of power their full potential has yet to be realized and argued that cyber has not been fully integrated at the tactical level into ground force combat doctrine. At the strategic level, the study noted, cyber plays a role in the multidimensional offensive capabilities envisaged in the IDF's current five-year plan (*Tnufa*), although an overall operational concept, critical to the IDF's ability to fully realize its cyber potential, has yet to be formulated. The study further found that the IDF had not fully realized the cyber realm's potential contribution to the conflict with Iran, nor fully appreciated its significance as a means of manifesting Israeli power in general.[22]

Some former senior officials share the sense that Israel has not fully realized the potential of its offensive cyber capabilities,[23] including a failure on the part of the IDF to sufficiently define its objectives in the cyber realm and develop a truly comprehensive plan integrating both cyber and non-cyber means of achieving them.[24] Others believe, more optimistically, that the IDF can cause cyber effects of systemic consequence to adversaries or at least inflict far-reaching disruption on critical national facilities, military capabilities, and economic and governmental systems.[25] "If we have a cyber vision, a willingness to fantasize, cyber can enable us to achieve a change in the rules of the game. If the vision is set, the 18-year-olds will find a way to do it."[26]

Unsurprisingly, there is a gap between what some former senior cyber commanders believe Israel is capable of and the views of some of the ultimate decision-makers.[27] One question is whether the state of the technology today is sufficiently advanced to achieve truly systemic, or even sustained major, effects. Systemic effects require the ability to maintain persistent engagement with a significant investment of resources, much like the difference between limited air attacks and an entire air campaign, and this is difficult to do in the cyber realm. Cyber can certainly cause significant damage, but more focused attacks, rather

than attempts to achieve systemic effects, may actually result in the greatest disruption in practice.[28] Whatever the case, Chief of Staff Kochavi stated that the IDF operations that had changed the most in 2020 were those in the cyber realm, in which it had conducted numerous offensive operations.[29]

Israel's offensive cyber operations are constrained by two primary considerations. First, there is the danger that continuous engagement may expose Israel's unique capabilities to its adversaries and consequently undermine its cyber superiority. Cyber capabilities can be replicated relatively easily, and truly advanced ones are best kept for the appropriate time, not squandered through ongoing day-to-day friction.[30] Second, there is the risk of retaliation and escalation and even of a prolonged cycle of cyber attack and counterattack. The cyber realm is still relatively new, the rules of the game and international law have yet to be established, the international reaction may be significant, and Israel is concerned that it knows how cyber confrontations begin but not necessarily how they end. Maybe most importantly, Israel's cyber dependence is greater than that of its enemies.[31] Given these considerations, Israel has become more judicious over the years in its approach toward offensive cyber operations, moving from an emphasis on more and more operations to greater caution.[32]

The IDF's approval process for cyber operations is similar to that for kinetic operations. Standard operating procedures set the parameters for cyber intelligence collection processes and defensive responses, without the need for further approval. Offensive and information operations, conversely, require the approval of the chief of staff, defense minister, and even prime minister.[33]

The IDF is in the middle of an ongoing process of digital transformation, dubbed Networked IDF, which links all of its forces (ground, air, sea, and intelligence) through one cloud-based military network. The new system is designed to provide for much faster and more effective "intelligence-based combat" against multiple targets; improve inter-service integration and command and control from the general staff down to junior commanders in the field; collect more reliable information about the damage actually caused; and minimize both friendly fire and collateral damage.[34] In 2020, as part of the Networked IDF, a new 1.6 billion shekel (approximately $450 million) cloud data center, David's Fortress, was opened. The highly secure facility, several floors below ground, is slated to meet the data storage and processing needs of all IDF combat forces for 50 years.[35] To give one partial indication of the extent of the data stored, Military Intelligence (MI) alone collects 10 terra bytes of information from aerial reconnaissance and image sorties during each day, 1 billion cellular phone acquisitions, 2 million pictures and half a million email exchanges.[36]

The Networked IDF system was first used, in a less advanced form, during the conflict in Gaza in 2014. By 2021 the system employed AI and advanced vision technology to integrate complex intelligence from multiple sources, provide

commanders with real-time views of the battlefield, prioritize targets, and identify the units best tasked with attacking them.[37] Needless to say, Networked IDF also creates a vast new "attack surface" for adversaries and a potential source of vulnerability that the IDF must defend.[38]

Deficient cooperation and conflicts of interest between IDF units using dissimilar infrastructure, reportedly continues to prevent true "jointness,"[39] despite the Networked IDF. Nevertheless, a prominent study of the 15 most cyber-capable states in the world, found that the IDF was second only to the United States in 2021 in deploying cyber capabilities throughout its force structure. It also concluded, however, that no state, Israel included, had yet made a complete transformation of its armed forces to well-integrated and broadly dispersed cyber capabilities, thereby indicating that the full potential of military cyber power has yet to be realized.[40]

The IDF conducts offensive cyber exercises regularly, in addition to the defensive exercises it has conducted together with the relevant civil agencies since as early as 2012.[41] In 2015 IDF cyber forces were fully integrated into a three-day general staff exercise, along with the air force, navy, and ground forces, designed to assess how rapidly Israel's cyber defenses could be mobilized, as well as their efficiency under emergency conditions.[42] The 2020 annual exercise simulated a multi-front war in which cyber attacks were employed to suppress enemy capabilities to a heretofore unprecedented extent.[43]

In the absence of a comprehensive military cyber doctrine, the IDF has not formulated a systematic methodology for determining whether to respond to cyber attacks by cyber or kinetic means, or whether to use them to conduct offensive operations. Instead, decisions are made on an ad hoc basis, depending on the situational context, nature of the target, and range of capabilities available.[44]

Cyber Defense Is Critical Too—much as defense has become an important component of Israel's overall strategic thinking in recent decades, adding a new fourth pillar to the traditional military strategy of the 3Ds (Detection, Deterrence, and Decisive Defeat), so too has Israel come to attach great importance to defense in the cyber realm. Indeed, considerable concern exists that Israel's military cyber sector, much like the civil, remains insufficiently defended.[45]

The former commander of one of Israel's most critical military capabilities had trouble sleeping at night. "Cyber could be used to cause systemic damage and to neutralize Israeli capabilities of strategic importance. Unlike kinetic capabilities, the cyber world can cause a complete loss of one's offensive capabilities, all at once, maybe without your even knowing about it." He further believes that the cyber threat "confronts Israel with its national DNA and mindset," which has always been offensive minded but must now internalize the need to emphasize

cyber defense. He himself defined cyber defense as the number one priority for his military command, even more important than its crucial offensive mission.[46]

A former cabinet minister, highly regarded for his strategic acumen, is also deeply concerned about the cyber threat to critical Israeli military capabilities, not just from enemy states but friendly ones as well. IAF aircraft, for example, are manufactured by the United States, potentially providing that country with the means to disrupt or even shut down operations of which it might disapprove. Israel's strategic capabilities may, similarly, be vulnerable to both enemies and allies.[47] The fear of cyber attacks by Israel's allies is not an idle one. As noted in Chapter 4, a joint US-UK cyber operation in the mid-2010s hacked encrypted transmissions from IDF planes and drones in order to monitor Israel's operations in Gaza and the West Bank and, even more worryingly from Israel's perspective, possible preparations for an airstrike on Iran's nuclear program.[48]

Preventing a cyber attack is usually far easier than dealing with the consequences once a network has been breached. Intelligence and early warning (detection) are thus crucial components of Israel's cyber defense operations and of the ongoing battle to stay at least a few steps ahead of adversaries. They are not, however, always sufficient and the next level of defense includes strong capabilities designed to counter threats by adversaries who may have spent years and devoted great resources to planning attacks. A third level of defense is provided by cyber intervention units, whose job is to identify the origin and nature of an apparent attack and confirm that it either has, or has not, taken place.[49]

The IDF's working assumption is that adversaries have succeeded in penetrating its systems. Indeed, 10% of all failures in IDF computer systems in 2016, including operational and classified ones, were reportedly the result of cyber attacks, or suspected ones.[50] In a 12 month period between mid-2021 and mid-2022, the IDF successfully thwarted tens of Iranian attacks against military computer systems. Some of the attacks focused on the electromagnetic spectrum used by IDF units.[51]

The Cyber Defense Brigade thus scours IDF computer systems and networks to seek out and find weaknesses before enemies can exploit them. In one case in 2018, apparently involving Hamas, a cyber intervention team was sent to the Gaza border to determine whether a computer system had been breached. It turned out that a problem did exist, and the team was able to address it on the spot. The Cyber Defense Brigade also employs "red teams" to simulate attacks by highly capable adversaries and conducts surprise drills in IDF units to strengthen commanders' awareness of the threat and improve their responses.[52] The ISA, similarly, uses hackers who try to penetrate the computer systems of public and private institutions, such as banks, hospitals, the national water company, and others, in order to expose and address potential vulnerabilities in advance.[53]

The Cyber Defense Brigade operates a 24/7 "cyber situation room," staffed by cyber defenders and intelligence personnel and located in an underground facility several stories deep, designed to enable it to function fully even while under severe kinetic attack.[54] The IDF's top cyber defense priorities are reportedly enemy attacks against C4I systems, anti-rocket and anti-missile systems, such as Iron Dome and Arrow, and air control radar, including attempts to overload them with images of hundreds of fake aircraft.[55]

The IDF has repeatedly succeeded in thwarting Hamas cyber attacks, including fake dating and sports sites set up to induce soldiers to download malware onto their smart phones (see Chapter 4). In some cases, Hamas was initially successful in hacking the soldiers' phones and in gaining potentially valuable intelligence on IDF bases and force deployments in a sensitive region, and even live images of IDF war rooms. Nevertheless, a combination of practical measures instituted by the IDF to stop the attacks, including a special 24/7 hotline to which soldiers could report suspicious activity, together with programs to heighten their awareness of the dangers, proved effective. The IDF even conducted a sting operation of its own, similar to the attacks carried out by Hamas, to test and further increase soldiers' awareness.[56] To this end, IDF cyber security personnel assumed fake persona and sent "friend" requests to 350 soldiers; 6% accepted the requests and received warning emails in response, others reported what they considered to be suspicious activity.[57]

In another well-known case, following a botched IDF intelligence operation in Gaza in 2018, Israel blocked all access to Hamas websites by Israelis. Given the sensitivity of the operation, this highly unusual step was taken in order to prevent further dissemination of the pictures of the IDF soldiers involved and to prevent Hamas from using social media as a means of eliciting additional information about the unit and the operation from unsuspecting Israelis.[58] Little bits of information gathered from large numbers of people, each of whom might know some otherwise minor detail about the soldiers and unit involved, could have added up to a deeply disturbing intelligence composite.

Upon occasion, the Cyber Defense Brigade also provides assistance to civilian targets. A prominent example was the assistance it provided to the Hillel Yaffe hospital, to recover from an Iranian-affiliated attack that caused severe damage to its computer systems in 2021.[59]

Beyond all this, little is known of Israel's offensive and defensive military cyber doctrine and how it fits into its overall national security and military strategies. To illustrate, no formal statement has been made regarding such questions as the conditions under which Israel would conduct cyber attacks, the factors that would determine whether its responses would be limited to the cyber realm, or whether it might adopt an approach of "no first use" of cyber. Nor has Israel

defined what defeat of the enemy and military decision constitute in the cyber realm.[60]

Nuclear Dilemmas

A further question of significance is what role, if any, cyber weapons might play in Israel's broader set of strategic capabilities, including its purported nuclear ones. To this end, a few words are in order regarding some of the dilemmas that Israel's nuclear strategy may face, primarily as background for some of the recommendations appearing in the final chapter.[61]

Israel's nuclear strategy, as explicated in Chapter 6, is based on a long-standing policy of nuclear ambiguity, in accordance with which it neither acknowledges nor denies having nuclear weapons. The nuclear strategy also has a preventative component, known as the Begin Doctrine, whereby Israel will prevent any hostile state in the Middle East from acquiring nuclear weapons, by whatever means necessary. To date, the doctrine has been implemented in practice against the nuclear programs of Iraq (1981) and Syria (2007).

The Begin Doctrine may, however, have now run its course. In the early 2010s, at a time when both the prime minister and defense minister were reportedly considering a military strike against Iran's nuclear program, the IDF chief of staff, head of Mossad, and other defense chiefs, were strongly opposed, especially if conducted without US approval.[62] Whether for that reason or not, the Begin Doctrine has not been implemented so far against Iran, at least in the classic sense of an air strike, although the numerous kinetic and cyber attacks that Israel has reportedly conducted to sabotage, delay, and derail Iran's nuclear program may be a new means of implementing it. Some reports have referred to targeted killings of Iranian nuclear scientists, others to explosions at Iranian nuclear and missile sites. The Stuxnet virus, reportedly a joint US-Israeli covert cyber attack in 2010 (elaborated on later in this chapter), which led to the destruction of Iranian nuclear centrifuges and to the postponement of the Iranian program,[63] is the most famous of these efforts.

It is, however, increasingly questionable whether Israel will be able to implement the Begin Doctrine in the future, by kinetic means, should one or more of the likely regional nuclear proliferators—Turkey, Saudi Arabia, and Egypt—actually decide to pursue military nuclear programs. All three countries are US allies and enjoy, to varying degrees, a US commitment to their security. Turkey is even a member of NATO and thus a beneficiary of its collective security guarantee. Further complicating the picture, Israel has diplomatic and economic relations with Turkey, as it does with Egypt, with whom it has been at peace for

over four decades. Israel reportedly also has been expanding ties in recent years with Saudi Arabia, with whom it shares a vitally important perception of the threat posed by Iran.

Were Iran, or one of these other potential proliferators, to pursue, or actually achieve, a nuclear capability, a cascading effect is likely to result, with others following suit. A Middle East with multiple nuclear actors is a nightmare scenario, for which there are no good answers and which Israel certainly seeks to avert. The other options available to Israel for addressing this dramatic eventuality, other than preventative military action, might include a defense treaty with the United States or regional arms control agreements. Both have significant drawbacks and feasibility questions of their own. Even assuming that these options were implemented, they could, at best, mitigate the severity of the threat, not resolve it.

In the coming years, Israel may thus have to reconsider its nuclear strategy and the options available to it. Nuclear ambiguity, which has been extraordinarily successful as the ultimate guarantor of Israel's security for half a century, along with airstrikes to implement the Begin Doctrine, may no longer be the most effective approach during the coming decades. Indeed, Stuxnet and the related attacks attributed to Israel (see later in this chapter) may have been an early indication that it has already begun to seek a cyber alternative to the Begin Doctrine, which is focused on kinetic action. The question Israel faces today is if and to what extent cyber may add critical new tools to its strategic capabilities.

The 2018 US Nuclear Posture Review raised the harrowing and almost unimaginable possibility, of the use by the United States of nuclear weapons in retaliation for a cyber attack that had caused massive loss of life.[64] The UK, too, has hinted at a similar response to a devastating cyber attack.[65] US academic experts, conversely, have expressed concern that the United States might be deterred from actually escalating to the nuclear level, in a case such as this, especially if the perpetrator of the cyber attack was also a nuclear power, such as Russia, China, or North Korea today or possibly Iran in the future. There is also the related fear of cyber attacks that disrupt US nuclear command and control systems and prevent it from being able to launch weapons, or delay this sufficiently to allow the attacker to first destroy US nuclear forces.[66] Israel's nuclear thinking would have to take issues such as these into account.

Cyber Units in the IDF, ISA, and Other Agencies

The cyber realm, unlike all other dimensions of military operations, is the only one in which the IDF does not bear sole responsibility for defending Israel from external threats, or even share responsibility for defense of the home front

(except in extreme circumstances in wartime). Whereas the IDF is responsible, for example, for defending the nation's critical infrastructure from external kinetic attacks, including terrorism and rocket fire, this is not the case for cyber attacks.[67] The IDF obviously works closely with the INCD and ISA and provides intelligence warnings of impending cyber attacks against public or private sector targets, but is not responsible for defending them and is not the lead operational agency.[68]

Cabinet Decisions 3611 and 2444, as well as the pending Cyber Bill (see Chapter 7), do not demarcate the roles of national security agencies in the cyber area, other than to emphasize that the legal and organizational changes provided for were not to detract from their existing areas of authority and responsibility. As a consequence, little is known about the statutory framework that governs the cyber operations of the IDF, ISA, and Mossad, or of the policy framework. The latter is embedded in a variety of classified internal policy documents, guidelines, and regulations.[69]

Responsibility for IDF cyber operations is divided between two primary general staff branches, the C4I and Cyber Defense Branch, and MI. The former is responsible for protecting the IDF's communications infrastructure and tele-processing systems, active defense, and achieving cyber superiority, inter alia, by providing the necessary professional expertise to MI, Unit 8200, and the Mossad, ISA, and INCD. The C4I and Cyber Defense Branch includes the Cyber Defense Brigade, an operational command responsible for defending the entire IDF against cyber attacks;[70] the Lotem Information Technology Brigade, responsible for operating the systems and networks used by combat, planning, and support units throughout the IDF;[71] and within Lotem, a unit of long-standing renown in Israel, the IDF Center for Computing and Information Systems (MAMRAM), which provides data and processing services for the general staff. MAMRAM also runs the School for Computer Professions (BASMACH), which trains recruits for positions in MI and other units that require sophisticated cyber skills.[72]

Within MI, Unit 8200, akin to the US National Security Agency or British National Cyber Security Center, has long born responsibility for signals intelligence, electronic eavesdropping, and code decryption.[73] Today, it is also responsible for cyber intelligence collection and offensive cyber operations. Unit 8200 reportedly focuses on data mining and especially the ability to analyze the mountains of information gathered in order to find recurring patterns of potential interest.[74] It also plays a vital, round-the-clock role in providing early warning of impending cyber attacks. To mention just a few of the publicly known cases, Unit 8200 played a key role in thwarting an ISIS attack on an Etihad flight from Sydney to Abu Dhabi in 2018, Iranian cyber attacks against public and private organizations in Israel, and dozens of Palestinian "lone wolf" terrorist attacks.[75]

In the mid-2010s the IDF devoted considerable attention to the organizational structure that it might best adopt in order to best address the rapidly growing cyber threat. Three primary organizational models were considered, all designed to concentrate offensive and defensive capabilities under one umbrella: creation of a new cyber command, giving MI authority for this, or doing so under an expanded C4I and Cyber Defense Branch.[76] In 2015, following extensive staff work and fierce, at times acrimonious, inter-service rivalry, the chief of staff decided to adopt the first model and establish a unified cyber command.[77] In 2017, however, two intertwined sets of considerations led him to backtrack and scrap that plan in favor of the existing organizational structure. First, lingering doubts about the preferable structure led to a decision to wait until the information necessary for a more mature decision had become available. Second, and probably even more important, the fierce bureaucratic politics that surrounded the original decision within the IDF, spearheaded by MI, had continued unabated.

MI was adamant that it could continue to fulfill its primary mission as the intelligence branch and also be the cyber command, with responsibility for all offensive and defensive operations.[78] For MI the issue was critical, almost existential, and it brought all of its considerable organizational clout to bear in order to force a change on the chief of staff. MI's concerns were primarily twofold: it feared losing the responsibility for offensive cyber operations that it had already gained and—far more importantly—even control over its largest and most prestigious organizational component, Unit 8200. Cyber intelligence operations, by this time, had become MI's primary means of intelligence collection and almost its organizational raison d'etre.[79]

MI's determination to head the new cyber command was opposed with almost equal fervor by others in the IDF and defense establishment who did not believe that it could effectively spearhead offensive operations. Opponents feared that MI, as an intelligence agency, would accord primacy to intelligence collection and the protection of sources at the expense of offensive cyber operations that might put these at risk.[80] Although MI had long been responsible for some operational missions, it was primarily a staff branch not an operational service, such as the air force or navy, and opponents further feared that it lacked the necessary "killer instinct." They thus favored establishment of an independent command responsible for both cyber offense and defense, with MI continuing to provide the critical intelligence input.[81]

A further source of opposition to the changes made by the chief of staff stemmed from those responsible for cyber defense, who feared that a focus on collection and offensive operations would come at the expense of defensive ones and thus favored giving the organizational lead either to a restructured C4I branch or an independent cyber command.[82] Still others believed that in the

absence of an independent cyber command, no one in the IDF would truly be responsible for overall integration and planning of cyber operations, especially on the offensive side, and that the IDF would not be able to realize its full cyber potential.[83]

In the end, the chief of staff made do with a compromise that satisfied no one. Cyber defense remained under the C4I and Cyber Defense Branch and cyber intelligence and offensive operations under MI,[84] leaving the heads of the two branches as coequal commanders of separate offensive and defensive campaigns. To integrate operations, a Cyber Center was established in the general staff's Operations Branch,[85] but doubts remained as to whether its organizational stature was sufficient. Further complicating the picture, an unrelated organizational reform in 2020, which established a new Iran and Strategic Affairs Branch in the general staff, added another senior bureaucratic player to those already involved in the decision-making processes regarding Iran, the IDF's primary focus today. Former Chief of Staff Eisenkot, among others, remains convinced that a unified cyber command will ultimately prove essential.[86]

The ISA was the first defense body in Israel to establish a dedicated cyber unit, the National Information Security Authority (NISA), which was charged with defending critical national infrastructure from cyber attack and with simulating attacks to ensure Israeli preparedness.[87] Following the establishment of the INCD, responsibility for protecting critical infrastructure was transferred to it, with the exception of the telecommunications sector, which remains under ISA. In recent years, the ISA has established a new Operational Technology and Cyber Branch, merging three preexisting branches: SIGINT (signals intelligence), Technology, and Cyber. The new branch is responsible, inter alia, for promoting greater integration within the intelligence community and between it and the INCD.[88]

The "cyber revolution" came to ISA at least partly in response to two severe national and organizational traumas, the assassination of Prime Minister Rabin and later the massive wave of terrorism during the second Intifada (Palestinian uprising). The former led to a fundamental reassessment of ISA's role and to a decision to replace its long-standing reliance on Humint (human intelligence) with cyber means. The Intifada similarly led to the recognition that a major intelligence effort was necessary to track potential terrorists through computer networks and cellular phones. The cyber revolution did not come easily to the ISA. Bureaucratic battles between different branches prevented agreement on the necessary changes, and it was only in 2009 that the above mentioned Operational Technology and Cyber Branch was established, along with a cyber department in all other branches.[89]

Over the years, ISA investment in technology and cyber has skyrocketed. Indeed, one third of all ISA personnel in 2020 were reportedly engaged in cyber

and SIGINT, compared to only 4% in the early 2000s.[90] ISA devotes a great deal of effort today to open source intelligence collection from computer networks, social media, and telephone conversations,[91] combining big data mining techniques with secretive spying tools to achieve what has been reported to be previously unattainable synergies.[92]

The ISA reportedly also relies on sensors installed in critical telecommunications networks to detect cyber attacks before they occur, but without monitoring the substance of the communications in order to protect privacy rights.[93] It further conducts offensive cyber operations, mostly for purposes of counter terrorism, to establish deterrence and disrupt planned attacks.[94] The offices of the ISA's cyber unit, according to one press report, look more like a corporate high tech office, complete with espresso machines, PlayStations, Xboxes, sofas, and colorful designs, comparable to the work environments of high tech giants and designed to attract high quality young personnel.[95]

The Mossad has reportedly built extensive defensive and offensive cyber capabilities. In 2021 it underwent an important structural reform designed to greatly strengthen its cyber capabilities, including machine learning, big data, and artificial intelligence. It did this by splitting the former Technology Branch into three sub-parts: offensive cyber, technological infrastructure, and IT.[96] The offensive cyber branch was to be devoted to cyber operations and its success measured solely on the basis of its success in that area.[97]

The Ministry of Defense's internal security department (MALMAB) is responsible for protecting it and its subordinate defense industries from cyber and other threats.[98] The Ministry of Foreign Affairs has an Algorithmic Diplomacy Team that deals with fake stories and posts and brings them to the attention of the social media companies.[99] It also has an official responsible for international diplomacy in the cyber realm. The Ministry of Justice has departments dealing with cyber legislation and international law,[100] and the Israel Police have a national cybercrime unit.[101]

As with other asymmetric threats, maybe even more so, delineating organizational responsibilities in the cyber realm has proven to be particularly challenging. The deputy head of the ISA even believes that the organizational boundaries and hierarchical command processes that were effective on the battlefields and in counterterrorism operations of the past are obstacles in the cyber realm. Attempts to delineate organizational responsibilities by defense, offense, geography, or type of intelligence to be collected are inappropriate to the cyber realm, he believes, in which attacks may begin in an enemy state, be directed through servers in friendly states, and then enter Israel in disguise. Matters are further complicated by the need for algorithmic compatibility between the different organization's computer systems, as well as for continuous and extremely precise flow of information and close coordination of force buildup measures.

Existing mechanisms for coordination and cooperation, he believes, are particularly deficient when it comes to information operations. Cyber thus requires greater inter-agency agreement on objectives, responsibilities, and priorities and a greater synchronization of efforts, so as to turn them into one effective whole.[102]

Cyber threats begin in what is known in Israel as the red zone (foreign territory, friendly or otherwise) where sovereign governments predominate; pass through the white zone (the Internet) where major multinational corporations predominate; and then enter the blue zone, Israel, where public and private entities predominate.[103] The INCD is responsible for providing public and private sector entities, that is, those in the blue zone, with early warning in regard to cyber threats and overall guidance for cyber defense, robustness, and resilience. When it comes to actual prevention and defense against cyber threats in the blue zone, the Mossad and IDF are responsible for defending against *enemies*, ISA and MALMAB for *adversaries*.[†] In the red zone, the IDF and Mossad are responsible for providing defense against cyber threats stemming from *enemies*, ISA for *adversaries*. The white zone is a shared area of responsibility in terms of early warning, in which none of the organizations has a solo mandate.[104]

No agency has been given formal responsibility for leading and integrating Israel's overall military efforts in the cyber realm, in peace time or wartime.[105] Informal understandings between the agencies have assigned the IDF with responsibility for overall operational integration of the cyber campaign during wartime,[106] as in other fields, but this has not been formally sanctioned by the political leadership or in statute.[‡]

In the absence of a formal determination, the ISA has chaired an informal inter-agency coordinating mechanism in recent years, comprised of representatives from the C4I Branch's Cyber Defense Brigade, Unit 8200, the MoD (MALMAB), and the INCD. During military crises, the head of the Cyber Defense Brigade assumes the lead, in keeping with the above agreement. In addition to ongoing daily exchanges between the various organizational participants, the forum meets on a weekly basis to discuss the cyber intelligence picture, formulate policy, and decide whether and how to respond to attacks. Each agency contributes its own unique capabilities for purposes of early warning, prevention, disruption, and defense, and tasks are assigned accordingly. The forum started as the personal initiative of a number of officials who felt the need for this type of interagency forum. Over the years it has reportedly proven to be highly effective,[107] but its semi-voluntary basis and consequent lack of formal

[†] Enemies refer to actors such as Iran, Hezbollah, and Hamas. Cyber adversaries refer to otherwise friendly states, such as Russia and China.

[‡] Figure 10.1 presents the Israeli government's overall organizational structure and division of authority for cyber affairs.

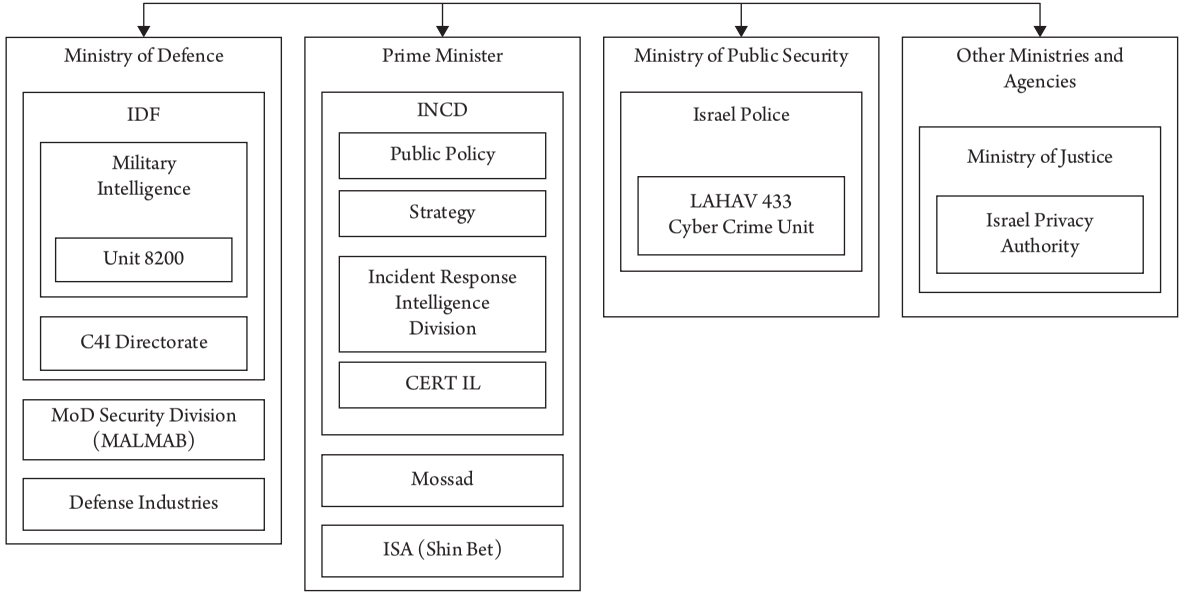


Figure 10.1 Israel's Cyber System Source: Adapted from Frei 2020

structure remain a primary weakness. A few tens of IDF soldiers from the C4I Defense Brigade are stationed at ISA to facilitate smooth communication and cyber security cooperation between the two agencies.[108]

Cyber Attacks Attributed to Israel

Since the early 1990s, the United States and Israel have engaged in a variety of joint efforts, diplomatic, economic, and military, designed to prevent Iran from acquiring nuclear weapons. The cyber realm has reportedly been a key component of these efforts, of which the Stuxnet attack on Iran's nuclear centrifuges may have been the high point. Stuxnet was actually just the best-known part of a far broader operation dubbed Olympic Games. Israel has not formally acknowledged involvement in Stuxnet, despite extensive media reporting and even confirmation by the United States that it was a joint operation.[109]

Israel has, of course, also conducted independent cyber operations, as well as two kinetic attacks against Hamas cyber capabilities. The following section describes what is known of these operations. With the exception of Olympic Games, the available details are limited, but clearly demonstrate the great emphasis that Israel's strategic culture has always placed on offense.

Olympic Games —was a series of cyber espionage and sabotage attacks designed to disrupt and delay the Iranian nuclear program, possibly even derail it, in the hope that a diplomatic solution could be achieved.[110] As such, Olympic Games complemented ongoing US efforts to ramp up international diplomatic and economic pressure on Iran, along with an ever-present threat of military force, in order to force it to come to terms.

Olympic Games had four primary components, three of which were actually carried out, Flame, Duqu, and Stuxnet, as well as Nitro Zeus, which was planned but never executed. Olympic Games reportedly began under President Bush in 2005 and continued under President Barak Obama until its discovery in 2012.[111] Primarily a US and Israeli operation, the Netherlands, Germany, and possibly France also took part and made important contributions.[112]

Olympic Games was motivated by the Bush and Obama administrations' deep concern over the ramifications of a possible unilateral Israeli strike against the Iranian nuclear program, which they feared almost as much as the program itself. Israel had already bombed the Iraqi and Syrian nuclear reactors in the past, as part of the Begin Doctrine,[113] and for a period spanning much of the Bush and Obama administrations was actively signaling that it might do so again should diplomacy fail.[114] Among the indications of Israeli intent were a request in 2008 to purchase high powered bunker busting bombs, which Bush rejected,[115] and

a series of statements by senior Israeli officials, apparently including Defense Minister Barak, especially between 2010 and 2012.[116]

Bush and later Obama feared that an Israeli attack might cause a regional conflict, with potentially severe repercussions for US interests, and possibly force the United States to intervene. Both thus calculated that a cyber campaign of unprecedented type and scale, conducted in coordination with Israel, might be sufficient to forestall the Israeli need to attack[117] and minimize the regional and international fallout.[118] Obama is said to have believed that if Olympic Games failed, there would have been no time for sanctions or diplomacy, and Israel would have attacked.[119]

Important figures in Israel shared the US concerns, part of a deep and at times rancorous debate among top policymakers that played out both behind the scenes and, remarkably, on the front pages of the nation's newspapers. The head of the Mossad, Meir Dagan, was the most vociferous opponent of a military strike among Israel's defense chiefs, but the IDF chief of staff and the head of the ISA were similarly reticent, without at least implicit US approval.[120] Dagan feared that a military strike would postpone the Iranian program by no more than a matter of months, reinforce Iran's determination to acquire nuclear weapons, push it to bury the program so far underground that it would become essentially impregnable, and end up actually accelerating the weapons development process. An attack, he later told an interviewer, "would unite the Iranian people behind the project and enable (Supreme Leader) Khamenai to say that he must get a bomb in order to defend himself against Israel. Bombing would be the stupidest thing we could do." Dagan thus shared Obama's hope that Olympic Games would achieve the desired delay in the Iranian program, without the condemnation, retribution, and escalation that would have almost certainly followed a kinetic attack.[121]

Prime Minister Netanyahu and Defense Minister Ehud Barak reportedly sought cabinet approval for an attack on at least three occasions, in 2010, 2011, and 2012, but apparently failed to muster the necessary majority when faced with the united opposition of virtually the entire defense leadership. Toward the end, Barak himself seems to have backed away from his earlier support for an attack and it is not inconceivable that Netanyahu, who had successfully forced other difficult positions through the cabinet but is known for military caution, may have done so as well, his strident public posture notwithstanding.[122]

The NSA and CIA were the primary players in Olympic Games on the US side, the Mossad and Unit 8200 in Israel.[123] The cooperative effort was not without tensions, both over tactics and strategy. In one case in 2012, Iran uncovered a series of cyber attacks on its oil industry, which the United States publicly blamed on Israel.[124] The overall outcome of the joint effort was, nevertheless,

an unprecedented cyber campaign, starting with Flame, followed by Duqu, and culminating in Stuxnet.[125]

Flame —was a highly complex cyber intelligence operation designed to collect information about Iran's nuclear program and a precursor to the centrifuge sabotage program conducted under Stuxnet. Flame may have started as early as December 2006 and may have lasted for over five years, continuing to gather intelligence in support of Stuxnet even after the sabotage program had begun.[126]

Flame was able to take control over computers and smartphones and use their built-in microphones and cameras to record audio and video, take screenshots of specific applications, log keyboard activity, capture network traffic, and send and receive commands and data. Dressed up to look like a legitimate Microsoft update, it was actually a backdoor Trojan horse.[127] Likely introduced via a USB stick, once the initial computer had been infected, Flame was able to spread across a local network without further instructions. To reduce the risks of discovery, it was also able to determine the type of antivirus software installed on a computer and modify itself accordingly.[128] Flame did not, however, have the ability to replicate itself automatically[129] and could only infect computers that had been knowingly targeted.[130] Flame was modular, meaning that it could be programed for a variety of different uses and new uses could be added over time.[131]

In addition to the nuclear program, Flame targeted computers at Iran's Ministry of Petroleum, National Iranian Oil Company, Iranian Offshore Oil Company, Central Bank, and Ministry of Culture.[132] Although Flame focused on Iran, it also appears to have targeted thousands of computers across the Middle East and North Africa.[133]

Flame was discovered in 2012, following what some have claimed may have been an independent Israeli cyber attack, conducted without the United States, during a period in which the negotiations with Iran had stalled.[134] Whatever the case, once discovered, Flame issued a preprogrammed "kill" command, designed to remove all traces of the infection from the targeted computers.[135] Despite its discovery, Flame is considered to have been one of the most advanced cyber attacks to date.[136]

Duqu —like Flame, was an espionage tool and a further precursor to Stuxnet,[137] but appears to have been more narrowly focused on a smaller number of targets.[138] Apparently first deployed in 2010, Duqu shared many features with Stuxnet,[139] including similar command and control protocols and architecture,[140] but was designed solely for purposes of intelligence collection, not sabotage.[141] Duqu lacked the ability to self-replicate, so that each targeted computer had to be infected individually,[142] but was capable of downloading additional modules and functionality.[143]

When infected documents were opened, Duqu utilized a zero-day exploit found in Microsoft Word to insert Trojan horses into targeted systems.[144] Duqu stole design documents, digital certificates, private keys (central to cryptography), and passwords, captured keystrokes and screenshots, and more. In preparation for Stuxnet, Duqu specifically sought out information about the industrial control systems[145] used in Iran's nuclear program. Once discovered in 2012, the server Duqu operated from was quickly shut down, and it largely removed itself from infected computers.[146]

Duqu 2.0, deployed in 2015,[147] was considerably more advanced than its progenitor, using three zero-day exploits,[148] and was likely spread via a spear phishing attack.[149] Duqu 2.0 infected the smartphones of the Iranian negotiators at the nuclear talks,[150] as well as the security cameras in the hotels they were staying in. Like Flame, Duqu 2.0 also appears to have targeted a wide range of systems in the Middle East and North Africa, as well as in Asia, Russia, and the West.[151]

Duqu 2.0 appears to have been self-replicating, that is, capable of spreading to any computer on a network. By stealing information and escalating access privileges, Duqu 2.0 ultimately moved its way up to the most secure and important computers on the targeted network and used Microsoft Windows Installer Packages to infect them with malware.[152] Duqu 2.0 operated from the targeted computer's volatile (temporary) memory, which is erased when the computer is turned off, rather than by downloading files, thereby making it harder to detect and enabling it to disappear without a trace.[153]

Stuxnet —the heart of the Olympic Games program, was the core malware reportedly designed by the United States and Israel to sabotage and delay Iran's nuclear program.[154] Work on Stuxnet likely began in 2005, and it may have been deployed as early as 2007. It was discovered in 2010.[155] Stuxnet is considered the first confirmed case of a cyber attack that caused physical damage and, as such, a turning point in the history of cyber conflict.[156]

Stuxnet targeted the computer and industrial control systems running Iran's nuclear centrifuges, the highly sensitive equipment needed to enrich uranium.[157] Nuclear centrifuges spin at supersonic speeds, and even minute fluctuations can make them crack and disintegrate. Stuxnet was thus programed to cause fluctuations in their speed that would be imperceptible to the human eye, including Iran's nuclear operators,[158] but also to insert recordings of normal operations into the centrifuges' control and monitoring systems to make it appear that they were functioning normally.[159] Stuxnet also made frequent changes to the pattern of the crashes caused, to prevent the Iranian investigators from developing a clear picture of what had happened. The subterfuge served two purposes. The first was the obvious need for operational secrecy. The second was to undermine Iran's confidence in its nuclear capabilities and sow confusion by making it

appear that the centrifuge failures had been caused by flaws in controls, designs, and parts and by professional incompetence.[160]

Iran's nuclear networks were air-gapped, meaning that they had no connections to outside networks and therefore that it was particularly difficult to introduce malware into them. Early versions of Stuxnet were likely inserted into the Iranian networks by means of an infected USB stick, reportedly by an Iranian engineer working for Dutch intelligence. Later versions apparently turned the Iranian contractors, who supplied the industrial control systems used at the nuclear facilities, into unwitting couriers.[161] Once uploaded, no further commands were necessary,[162] Stuxnet was entirely self-replicating and autonomous and thus able to spread across the Iranian nuclear networks and infect other computers on its own.[163] The ease with which Stuxnet supposedly spread may have enabled the United States and Israel to map out and damage previously unknown parts of Iran's nuclear facilities and computer systems.[164]

Planning for an operation as complex as Stuxnet is a major undertaking, necessitating a large-scale investment of time, money, and highly skilled personnel, along with advanced technological and intelligence capabilities.[165] Stuxnet involved the use of two stolen digital certificates, a Windows rootkit (software that grants hidden privileges and access in Windows), the first ever created Programmable Logic Controller (PLC) rootkit, an extraordinary four zero-day exploits, and more.[166]

To design sophisticated malware like Stuxnet, the programmers also required highly detailed intelligence about the specific configuration of Iran's enrichment program and supporting computer systems.[167] How this information was obtained is not fully known.[168] Following Libya's decision to dismantle its nuclear program in 2003, however, the United States and Israel gained access to computers similar to those used by Iran and obtained information about them from manufacturers of various parts,[169] insiders, and third-party contractors around the world.[170] Intelligence gathered from Flame and Duqu presumably also constituted a crucial part of the effort.

To further ensure that Stuxnet actually worked as intended, the United States and Israel reportedly built full-scale models of Iran's nuclear configuration at the Oak Ridge National Laboratory in Tennessee and at Israel's nuclear complex in Dimona.[171] The Iranian systems were replicated as accurately as possible with new features added over time as further information became available.[172] Later designs were expanded to anticipate generations of centrifuges and systems that Iran might choose to employ in the future.[173]

The United States and Israel were a good fit. While overall US intelligence capabilities are the most advanced in the world, Israel had areas of unique technical expertise and intimate knowledge of Iran's nuclear program.[174] Despite the exquisite planning and testing, however, Stuxnet escaped from the targeted

Iranian computers in 2010 and spread to roughly 100,000 systems in 115 countries.[175] None were adversely affected since Stuxnet had been programmed to only damage systems in Iran,[176] but its exposure meant that defenses could be built and that it could be copied and modified for use by others.

Stuxnet's escape was undoubtedly a major operational failure and a severe blow to US and Israeli hopes of disrupting the Iranian nuclear program. It can, however, also be viewed as an unfortunate reflection of the attack's otherwise brilliant conception and execution; part of Stuxnet's mission was to spread as far as possible and to gather information about previously unknown Iranian nuclear activities. That is exactly what it did. In the interim, Stuxnet succeeded in causing considerable havoc.[177]

Nitro Zeus —much less known is known about Nitro Zeus than the other parts of Olympic Games, in part because it was never carried out. It is also unclear what, if any, role Israel played in it.[178] Nitro Zeus was the cyber component of a broader campaign, Op Plan 1025, developed by the Obama administration in preparation for a possible war with Iran and designed to end that war even before it actually got under way, hopefully without having to fire a shot. Planning for the operation, to be implemented in the event that negotiations failed or that Israel launched an attack, began early during the administration.[179]

Nitro Zeus was designed to plunge Iran into darkness to give the United States and Israel time to bomb the suspected nuclear sites and hopefully make it impossible for Iran to strike back, thereby averting a larger war. Its core component was the insertion of both physical and cyber implants into critical Iranian networks and infrastructure at the onset of hostilities, including portions of the power grid, air defenses, communications systems, IRGC command and control systems, and missiles. Concomitantly, a cyber attack was to have been launched against the Fordow nuclear enrichment facility, which was buried deep inside a mountain and could only be destroyed with the most powerful bunker buster in the US arsenal. Unlike Stuxnet, which sought to conceal itself, Nitro Zeus would overtly destroy the circuitry powering the centrifuges at Fordow and their controllers. The plan also involved preparations for kinetic operations, to be activated only if actual warfare broke out.[180] Nitro Zeus became unnecessary when the nuclear deal with Iran was signed and the cyber attack was never carried out.[181] The Trump administration, however, continually updated the plans.[182]

Ramifications of Olympic Games —in the absence of detailed classified information, it is hard to provide an accurate picture of what the Olympic Games operations, including Stuxnet, actually achieved. Iran itself admitted that Stuxnet destroyed roughly 1,000 centrifuges and the Obama Administration claimed that it set the program back by about two years.[183]

The objective of sowing confusion and thereby making the Iranians overreact and even turn on each other was at least partially achieved. Indeed, Iran grew

so concerned by the centrifuges' failure rate that some of the most prominent nuclear scientists and engineers in the nation were fired[184] and many centrifuges were simply pulled out of operation to forestall further crashes.[185] A number of workers at the Natanz nuclear site, suspected of involvement in the attack, may even have been executed.[186] The fact that Stuxnet was only discovered after it had spread around the world, rather than by Iran's own defenses, added to the shock and further undermined Iran's confidence in the effectiveness of its security procedures.[187]

Whatever the actual delay achieved, the demonstration of US and Israeli resolve to prevent Iran from achieving nuclear capability heightened its sense of vulnerability, while strengthening US confidence in its ultimate ability to stop the program. As such, Stuxnet may have actually helped to reinvigorate the nuclear negotiations during 2012–2015 and create the necessary conditions for the deal that eventually emerged.[188] Stuxnet may also simply have been the best of the bad options available at the time. A military strike would have been difficult and would have led to a costly Iranian response, especially against Israel and other US allies in the Middle East, with potentially significant regional ramifications.[189]

Some critics argue that the delay achieved by Stuxnet amounted to no more than a matter of months, hardly an impressive outcome given the magnitude of the effort,[190] and that Iran ended up replacing the damaged centrifuges with more advanced ones.[191] In fact, by February 2010, while Stuxnet was active, Iran had advanced far enough to begin enriching uranium to 20%, a critical threshold for acquiring nuclear weapons,[192] and ultimately had some 18,000 operational centrifuges, approximately triple the number at the time the attack began. Rather than reinvigorating the negotiations, critics charge, Stuxnet may have dulled the US sense of urgency, as well as that of its partners, regarding the need to achieve an early resolution of the issue.[193]

Stuxnet's most consequential—and unintended—outcome may have been that it subsequently became the primary impetus for Iran's own cyber program. Having paid relatively little heed to the cyber realm up until that time, the deep shock caused by the attack led to a strategic decision on Iran's part to formulate a comprehensive national cyber strategy, including development of advanced defensive and offensive capabilities. A decade later, Iran is now thought to be at the top of the second tier of cyber actors and one of the more active and aggressive states in the cyber realm.[194]

More fundamentally, Olympic Games may have ushered in a new era of cyber conflict, with important ramifications for the future of diplomacy, espionage, and warfare.[195] Olympic Games, especially Stuxnet, provided leaders with new policy options for demonstrating resolve, deterring and coercing an adversary, and even causing damage without having to threaten or actually resort to the

use of force. They further demonstrated the ability to achieve military objectives with minimal risk and loss of life and even raised the heretofore unheard of possibility that states might be able to win wars without having to resort to kinetic force.[196]

Michael Hayden, former director of the NSA and CIA, may have said it best. Alluding to the first use ever of nuclear weapons, he stated in regard to Olympic Games that "this has a whiff of August 1945 . . . somebody just used a new weapon—and this weapon will not be put back in the box."[197] Unlike nuclear weapons, however, cyber weapons may prove to be a viable first-strike option.[198]

Operation Orchard —in 2007 Israel bombed and destroyed a nuclear reactor then under construction in Syria. The operation involved two separate cyber attacks. The first, a cyber espionage operation, sought to prove that the facility in question was a nuclear reactor. To this end, Israel reportedly installed a Trojan horse on the laptop of a senior Syrian official, who had left it in a London hotel room. The Trojan horse then sent detailed construction plans, pictures, and letters back to Israel, proving that it was, indeed, a nuclear facility.[199]

Once this had been confirmed, the IAF reportedly launched a second cyber attack to blind Syrian air defenses when it bombed the reactor. The cyber tool used appears to have been similar to BAE Systems' SUTER, which can take control of enemy networks and interrupt signals sent to weapons systems, such as surface-to-air missiles.[200] Using this cyber weapon, Israel apparently took over Syria's radar systems and tricked them into thinking that things were normal, even while the attack was underway. Israel chose not to shut down Syria's defenses, which would have alerted it to the fact that something was afoot, and instead temporarily reprogrammed them to make it appear that the system was functioning normally.[201]

In the years since Operation Orchard, Israel has reportedly conducted numerous airstrikes in Syria designed to prevent Iran from building up a military presence of its own there and using Syria as a transit point for shipping advanced weapons to Hezbollah in Lebanon. It is unknown whether Israel continues to use cyber attacks as a means of suppressing the Syrian air defense system.[202]

Bandar Abbas —the most advanced cyber attack attributed to Israel, other than Stuxnet and Operation Orchard, took place in 2020, in response to Iranian cyber attacks on Israel's national water system. Until then, Israel had successfully thwarted such attacks, but this time its defenses were breached, potentially allowing a poisoning of the national water system. Israel reportedly responded by escalating and launching a counter strike that led to an abrupt halt to shipping at a major Iranian port, Bandar Abbas, which handles nearly half of its overall foreign trade. Computer systems that regulate the flow of vessels, trucks, and goods all crashed at once, creating massive traffic backups and, according to at least one source, causing the port to be shut down for days.

The attack against the port was reportedly one of the middle-of-the-road options considered and part of a purported shift in Israeli thinking, from sparing use of cyber weapons to "constant cyber warfare," presumably a cyber expansion of the campaign between the wars. No one was to be harmed physically, but sufficient economic disruption would be caused to make Iran think twice in the future. Iran, however, was apparently not deterred; two further attacks on Israel's water system, albeit less severe, took place just weeks later.[203]

Cyber attacks attributed to Israel later in 2020 were launched once again against the port at Bandar Abbas and at least one other Iranian target, variously identified as the ministries of communications or transportation, the ports and shipping organization, customs service, and banks. Following the attacks, several Iranian governmental bodies temporarily shut down Internet services.[204]

From Parchin and Natanz to Regime Change? —about the same time as the first attack on Bandar Abbas occurred, a series of unexplained explosions, widely attributed to Israel, took place in Iran. The primary incidents occurred at a missile production facility at Parchin (also a suspected nuclear site) and the second, especially, at the Natanz nuclear centrifuge assembly plant. The attack at Natanz is thought to have matched the complexity and sophistication of Stuxnet, which struck an adjacent facility. Some Iranian officials initially claimed that the explosion at Natanz was the result of a cyber attack, but later reporting indicated that it was probably the result of an explosive device. Be that as it may, an explosion damaged a power plant in Ahvaz just two days later and there was a chlorine leak at a petrochemical plant in Mashar.[205]

In 2021 a different part of the Natanz facility was struck once again, causing significant damage. As in the previous case, initial reports claimed that the attack was conducted by cyber means, but still inconclusive reports subsequently indicated that it was more likely the result of explosions caused by kinetic means.[206] Just months later Iran's sole nuclear reactor was taken off-line for two weeks due to an unexplained "emergency," and a centrifuge manufacturing plant, for Natanz and the other primary enrichment facility at Fordow, was attacked, supposedly by drones.[207] If Israel was in fact behind the two attacks against Natanz, as well as the manufacturing plant, and if they were actually carried out by cyber means, this would indicate that Israel has, as suggested earlier in this chapter, adopted a new cyber approach to the long-standing Begin Doctrine of nuclear prevention.

In mid-2021, a group calling itself Ali's Justice hacked the surveillance cameras at Iran's infamous Evian prison and posted video clips on social media showing guards beating and abusing prisoners as well as fighting among guards and the prisoners themselves. Screens in the prison control room carried a message saying, "Evin Prison is a stain on the black turban and white beard of Iranian President Ebrahim Raisi, nationwide protests until the release of political prisoners." The breach caused a public outcry, leading the prosecutor-general to

call for "a comprehensive investigation" and to a humiliating public apology by the head of Iran's penal system.[208]

Also in mid-2021, a cyber attack against Iran's rail system caused temporary "chaos" and was followed the next day by an attack on the Iranian Ministry of Transportation.[209] Neither attack was directly attributed to Israel, but media speculation was that they were part of the ongoing shadow war between Iran and Israel.[210] Just a few months later, another attack disrupted sales at all 4,300 gas stations in Iran for nearly two weeks, causing long lines and frustration. The hackers sent digital messages to customers suggesting that they complain to Iran's Supreme Leader Ayatollah Khamenei and provided his office phone number. They also took control of billboards in major cities and replaced the ads with a message asking "Khamenei, where is my gasoline?" The hackers may have also gained control of the Oil Ministry's fuel storage tanks and access to data on international oil sales, which might have exposed how Iran evades international sanctions.[211]

At about this time, another cyber attack disrupted the website of Mahan Air, an Iranian airline sanctioned by the United States for its close ties to the Quds Force, the IRGC's secret arm for foreign operations, including transport of weapons and equipment for Hezbollah. In text messages to Mahan customers, the Defenders of the Homeland took credit for the attack and claimed to have obtained internal documents, emails, and reports showing the airline's connections to the IRGC. The hackers further claimed, Mahan's claims to the contrary, that the airline had never managed to shut down the attack.[212] Just days later, Iranian officials denied reports first aired on Iranian state TV that a series of cyber attacks had affected dams across the country.[213]

In early 2022 the above mentioned Ali's Justice hacking group briefly disrupted Iranian state TV. The broadcast was replaced with the image of a masked man saying that Iran's government "will no longer silence us. We will burn Hijabs. We will burn their pictures and propaganda posters . . . . We will reveal their palaces, so that the people can punish them."[214]

In mid-2022 the three largest steel factories in Iran were the target of a cyber attack by the same group that had conducted the attack the previous year against Iran's gasoline stations. The steel industry is one of the most important for the Iranian economy and the attack against the Khusetan factory, the largest of the three, was massive, forcing it to stop production for at least a few weeks. All three factories are affiliated with the Revolutionary Guards. At least one source suggests that the attack was in response to repeated Iranian cyber attacks against infrastructure targets in Israel.[215]

A variety of Israeli media sources attributed at least some of these attacks to an Israeli campaign designed to create popular unrest in Iran, put pressure on

the regime, and possibly even topple it, or at a minimum, pressure it to return to then suspended nuclear talks.[216] If true, Israel's actions may provide insights into the question raised in Chapter 3, whether or not cyber attacks can be used to force changes in policies, or even an entire governmental system.

Cyber Intelligence Attacks —cyber plays an increasingly vital role in Israel's intelligence capabilities, indeed, it is now the primary source of the intelligence collected.[217] In 2017 Israel reportedly succeeded in penetrating a small cell of ISIS bomb makers by cyber means, only to learn that they were developing explosives disguised as laptop batteries and designed to deceive airport screening machines. Israel provided highly detailed intelligence to the United States and UK, which led to a temporary ban on large electronic devices in carry-on luggage on some international flights.[218] In 2019 Prime Minister Netanyahu claimed that Israel's cyber intelligence had thwarted approximately 50 ISIS attacks in dozens of countries worldwide.[219]

No less dramatically, Israel reportedly alerted the NSA in the United States that Russian intelligence was using the antivirus software developed by Kaspersky, a Russian firm, to infiltrate sensitive systems in some two dozen US government agencies and that it was also using offensive cyber tools that could only have come from a breach of the NSA itself. In response, the Department of Homeland Security directed that Kaspersky software be removed from all US government computers. The alleged hack of Kaspersky's software was supposedly similar to the Duqu virus, but even more sophisticated. By using advanced cyber tools to steal passwords, take screenshots and vacuum up emails and documents, the attack succeeded in implanting multiple backdoors into targeted systems.[220]

Over the years, Hezbollah and Lebanon have accused Israel of various cyber attacks against them. In one such case, Lebanon claimed that Israel had hacked its cellular infrastructure for purposes of espionage.[221]

Kinetic Attacks against Hamas Cyber Capabilities —Israel has attacked Hamas's cyber capabilities, using kinetic means, on two occasions. Along with a US airstrike against ISIS in 2015, the Israeli airstrikes were precedent-setting—the first known cases of kinetic attacks against cyber targets.

The Israeli airstrikes, in 2019 and again during the round of fighting with Hamas in 2021, were launched in response to intelligence reports warning of a major and imminent cyber attack that Hamas was preparing to carry out. In the first case, the IAF destroyed Hamas's cyber headquarters and in the second it essentially destroyed its remaining cyber capabilities, including more than ten cyber operations rooms, a storage room for cyber equipment, an intelligence facility, and another facility used to try to jam Israel's rocket defense system, the Iron Dome. Hamas's cyber fighters were also targeted, including the head of its cyber operations, who was killed in what has been interpreted by some

as an indirect warning for Hezbollah's and Iran's cyber fighters. The attacks required close coordination between the C4I and Cyber Defense Branch, MI, and, of course, the IAF. In 2021, for the first time, artificial intelligence means were successfully used for targeting and other purposes in the course of this operation.[222]

PART IV

THE WAY FORWARD

Part IV is the very heart of this book, the reason we spent years writing it. Chapter 11 presents the primary conclusions derived from the Israeli experience in the cyber realm to date, both in the attempt to provide answers, to the extent possible, to the theoretical quandaries presented in Chapter 3 and as a model that other states can learn from. Chapter 11 is also designed to serve as a basis, together with all of the preceding background chapters, for our recommendations for a comprehensive Israeli national cyber strategy, presented in Chapter 12.

To avoid any misunderstanding, it is important that we reiterate what we already stated in the Introduction. The current and former officials interviewed for the book, agreed to do so in their private capacities and strictly on the basis of their personal views. The conclusions and recommendations in the following chapters are the authors' alone, based on the entirety of the research presented in chapters 1–10. They thus should not be misconstrued to reflect the views of the interviewees, or official positions. Similarly, none of the information presented throughout the book should be misconstrued to constitute confirmation of the events described, merely a summary of the publicly available record.

11

Conclusions—and Some Answers to the Cyber Quandaries

Sending special code is easier than sending special forces.
Professor Martin Libicki, cyber security expert

The changes wrought by the cyber realm are multifaceted—socioeconomic, political, military, diplomatic, technological, and even cultural—and they affect state and nonstate actors, organizations, and individuals alike. The ubiquity of cyber technologies and the critical role they play in nearly all walks of modern life mean that the cyber threat is not only very real but growing, as are the remarkable opportunities the cyber realm affords. We still do not know the full extent of the threat, nor where the opportunities will lead us. In some areas both our concerns and hopes will undoubtedly prove overblown, but they are significant and here to stay.*

Chapter 11 is divided into two halves. The first half seeks to provide at least some answers, based on Israel's experience in the cyber realm, to the theoretical and policy quandaries set out in Chapter 3. In so doing, it both provides important lessons for Israel and seeks to show how the Israeli experience can serve as a model for other states, as appropriate to their unique circumstances and capabilities. The second half addresses Israel-specific conclusions. We dub the answers in the first half findings and those in the second conclusions. Together, the findings and conclusions serve as the basis for the proposed national cyber strategy presented in the final chapter.

* Except where specifically indicated otherwise, the information presented in this chapter is based on information and citations already provided in the preceding background chapters.

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0012

Understanding Behavior in the Cyber Realm

Finding 1: The Realist and Constructivist Arguments, the Theoretical Bases for the Hypothesis, Were Substantiated

- Cyber Has Become a Critical Component of Israel's National Power and Strategy of Self-Reliance
- Strategic Culture Played a Major Role Shaping Israel's Decisions in the Cyber Realm
- Nonstate Actors Have an Important Impact on State Behavior in the Cyber Realm

The realist and constructivist arguments presented in the Introduction, the basis for the book's overall analytical framework and hypothesis, were clearly borne out in the Israeli case. In the face of an unusually harsh external environment, and in keeping with realist assumptions, cyber has become a critical component of Israel's national power and strategy of self-reliance and strategic autonomy, first and foremost, and its socioeconomic and military might, as well as an important part of its foreign policy. These changes reflect the fundamental transformation that has taken place in Israel's strategic landscape in recent decades: from conventional state-based military threats to asymmetric threats directed primarily against Israel's home front, by state and nonstate actors alike. As posited, cyber has thus been shown to have been both a strategic and socioeconomic necessity and opportunity for Israel.

Constructivism's emphasis on state identities and beliefs, including strategic and national cultures, helps explain the choices Israel made in responding to the threats and opportunities it faced. Israel's fundamental sense of insecurity led to a relentless quest to strengthen its national might, while advanced technological capabilities were considered a prerequisite for the qualitative edge with which to counter its adversaries' quantitative superiority. From the earliest days, Israel believed that it could only survive and thrive by developing advanced technological capabilities, with heavy investment in education, science, and technology. The cyber realm fit in particularly well with this long-standing approach.

Both Israel's civil and military sectors are deeply imbued with the national culture of improvisation, creativity, and innovation, what we have dubbed chutzpah gone viral, providing further support for the constructivist approach. The creative insecurity stemming from Israel's strategic circumstances, along with the compulsory military service that differentiates Israel from most other democracies, proved critical to the emergence of its exceptional cyber ecosystem and military cyber capabilities.

The importance Israel attaches to the "white zone," that is, the multinational tech giants that dominate the Internet, provides support for another constructivist claim: states are not the only actors that have a powerful influence on security issues and shape international relations. The tech giants have played an important role in shaping state behavior in the cyber realm, including that of Israel, and in creating the international environment in which states operate. Microsoft, for example, has been openly critical of Israeli sales of cyber capabilities to authoritarian regimes and Amnesty International, Facebook, and other nonstate actors have filed suits against one of the firms involved and the Ministry of Defense. The global backlash they helped generate against Israel's cyber export policy, following the NSO scandal, forced Israel to tighten controls. Domestically, the political battle over the proposed cyber bill illustrates the power that civil society actors have to shape laws.

Finding 2: Bureaucratic and Domestic Politics Had a Far Greater Impact Than Posited

- Repeated Cabinet Decisions Failed to Prevent Turf Wars between the Defense Agencies
- Within the IDF, Bureaucratic Warfare Was Even More Rampant
- Domestic Politics Had Deleterious Ramifications for the Civil Cyber Realm and Possibly the Military

Bureaucratic and domestic politics were found to have played a far greater role in the evolution of Israel's civil and military cyber strategies and institutions than posited. The cabinet decisions and cyber bill went to great lengths in the attempt to minimize bureaucratic politics, but to no avail. ISA fought the INCD at every step of the way, as did, to a lesser extent, the other agencies. Within the IDF, bureaucratic warfare was arguably even more rampant, ultimately undermining the decision to establish a unified cyber command. Bureaucratic politics at least partially account for the inability of both the INCD and NSS to play a sufficiently effective interagency coordinating role in the cyber realm, a critical function that has been only partly filled by the informal forum led by the ISA.

The Knesset's failure to enact the cyber bill, seven years (at the time of this writing) after the cabinet adopted the primary decisions in the cyber realm, Decisions 2443 and 2444, stemmed from a number of factors, including substantive controversy over the bill's provisions and the disarray caused by the Covid pandemic. It was, however, also a direct result of the ongoing domestic political crisis at the time and the consequent decision-making stasis.[†] To mention only

[†] Former Prime Minister Netanyahu's protracted battle to remain in office, despite the severe legal charges leveled against him and repeated inconclusive electoral outcomes.

a few of the deleterious ramifications for Israel's civil cyber realm and possibly the military as well: the INCD still does not exist in primary legislation and critical national infrastructure systems have yet to be legally defined; a number of gray areas remain in the division of authority between the governmental agencies responsible for the cyber realm; concerns continue to exist regarding civil liberties in the cyber realm; and important changes to the regulatory system await resolution.

These examples of bureaucratic and domestic politics affected not just the character of the decision-making process leading to the choices Israel made in the cyber realm but also the substantive decisions adopted. Bureaucratic and domestic politics were not, however, manifested to the extent that they challenge the fundamental validity of the hypothesis, which attributed primacy to the realist variables of strategic and economic necessity.

Finding 3: The Cabinet's Decision-Making Process Was Effective and Non-Politicized

- A Comprehensive Civil Cyber Strategy Was Formulated, Unlike Israel's Usual ad hoc Decision-Making Processes
- The Cyber Decision-Making Process Demonstrated the Strengths of Israeli Decision-Making
- The Decision-Making Process Was Especially Effective Compared to Other Asymmetric Threats Israel Has Faced

Bureaucratic politics and domestic political considerations had a significant impact on the decision-making process. At the cabinet level, however, the decision-making process was surprisingly smooth and effective, mostly substantive in nature, and lacking in the politicization so common to much Israeli national security decision-making. Moreover, a coherent and comprehensive strategy was formulated and adopted, in contrast with the ad hoc and atomistic character of most Israeli decision-making processes.

For the most part, the decision-making process leading to Israel's civil cyber strategy demonstrated the strengths of its national security decision-making process: the ability to improvise, change gears, and rapidly adapt to a new and evolving situation; pragmatic and problem-solving decision-making; and highly porous boundaries between the civil and military realms. Indeed, as we further note later in this chapter, Israel was one of the first states to develop a civil cyber strategy and an operational military doctrine, if not an overall military cyber strategy. The defense establishment initially brought the cyber issue to the cabinet's attention, and the interaction between it and the commercial sector

played a critical role in the subsequent development of Israel's cyber capabilities. To cite just one example, it was an informal group of IDF officers and business people who initiated the establishment of the first cyber courses in Israel, the basis for the more formalized programs later adopted in the educational system.

The cyber decision-making process at the cabinet level was especially effective in comparison with other asymmetric threats that Israel has faced over the decades, first and foremost terrorism, which it has had to deal with ever since the state's establishment and even before. To this day, Israel has not formulated and adopted a formal national counterterrorism strategy. Why there is such a pronounced difference between Israel's response to the cyber realm and other areas is an interesting question worthy of future research.

Finding 4: The 4Ds Model Does Apply in the Cyber Realm, but Needs Modification

- Many of the Concepts in Use Today to Understand the Cyber Realm Do Not Add Further Clarity
- There Is a Need for Theoretical Concepts Appropriate to the Cyber Realm's Unique Character

The classic model of military thinking discussed in Chapter 3, the 4Ds (Detection, Deterrence, Defense, and Defeat), with the addition of the newer concept of resilience, has proven useful in understanding both the theoretical and practical challenges facing cyber strategists. As will be explored in greater detail in the conclusions that follow, the first 3Ds and resilience do essentially continue to hold in the cyber realm, even if they are difficult to implement in practice. The fourth D, in contrast, Defeat, requires greater modification to address the specific qualities unique to the cyber realm.

We concur that there is a need, identified by many cyber scholars and practitioners, to adopt theoretical concepts appropriate to the requirements of the cyber realm. For the meantime, however, the plethora of concepts in use have not contributed to greater clarity. We conclude that the 4Ds model remains preferable until such time as the necessary new theoretical concepts have evolved.

Finding 5: Standalone Cyber Deterrence Is Impractical: Cyber Deterrence Requires a Multifaceted Approach

- Israel's Experience Demonstrates That Standalone Cyber Deterrence Is Impractical

- Israel Has Adopted a Combined Cross-Domain and Cumulative Deterrent Approach
- Israel's Deterrence Is Constrained by Its Cyber Dependency and Cyber Ambiguity
- Some Cyber Operations Have Been Transient and Even Counterproductive

Israel's experience demonstrates both the great difficulty that states encounter in trying to achieve effective deterrence in the cyber realm and that standalone cyber deterrence is essentially unattainable. This has clearly been the case of CNA attacks and is also true for CNI attacks, though less conclusively possibly due to the limitations of the available data. Throughout history, states have generally been unable to deter CNE attacks, whatever the technology of the time.

Of the three components of effective deterrence—capability, credibility, and communicability—Israel enjoys just the first two. Its cyber capabilities are advanced and credible, but Israel's ability to communicate their nature to its adversaries, along with its intentions and the consequences they are likely to suffer, is constrained by the broader foreign policy and military considerations that have given rise to the approach of cyber ambiguity. Israel's cyber deterrence is further constrained by considerations of operational secrecy, that is, the need to avoid exposing the vulnerabilities it may wish to exploit in future attacks; a presumed decision to hold some capabilities in reserve for wartime or other critical uses; and the awareness that Israel is considerably more cyber dependent than its adversaries and thus more at risk in the event of further escalation.

An *explicit deterrent* posture would risk exposing Israel's capabilities and is incompatible with cyber ambiguity. *Indirect deterrence*, based on general familiarity with the size and strength of Israel's cyber ecosystem and presumed military cyber capabilities, has not proven sufficient to date. It is unknown what, if any, *quiet deterrent signaling* measures Israel may have undertaken, but both they and s*ymmetric responses* are unlikely to prove effective, given the fundamentally hostile intentions of some of Israel's adversaries toward them.

In these circumstances, Israel views cyber deterrence as part of a broader approach not a standalone concept. It has thus adopted a combined deterrent posture, based on the dual concepts of cross-domain and cumulative deterrence, that is, application of the full range of capabilities available to it (cyber, kinetic, diplomatic, and economic) and a long-term effort to consistently frustrate attacks, to the point that its adversaries are ultimately dissuaded from trying further. To this end, Israel has reportedly conducted cyber and kinetic attacks both for purposes of deterrence by denial (e.g., Stuxnet, Operation Orchard, and airstrikes against Hamas cyber facilities) and retaliation (e.g., the attack against Iran's leading seaport).

In most cases, the deterrent effects of the various operations have proven to be transient, and some have had negative and even counterproductive consequences, such as Iran's decision to develop its own cyber capabilities in response to Stuxnet and possibly the ongoing exchange of blows between Israel and Iran since 2020. It is further noteworthy that Israel has assiduously refrained from declaring "red lines" in the cyber realm, much as it has generally done in regard to attacks in the physical world. This practice draws on the apparent assumption that in the deeply hostile and conflictual Middle Eastern environment red lines blur and tend to be rapidly erased. An understanding of Israel's red lines can thus only be surmised from its actual behavior over time.

Finding 6: Cyber Detection and Attribution Are Challenging, but Not Insurmountable

- Israel's Experience Demonstrates the Importance of Cyber for Detection and Early Warning
- Cyber Has Become the Basis for Intelligence-based Warfare, the "Campaign Between the Wars," and Broader Strategic Purposes
- Attribution Has Not Been a Critical Challenge and Is Likely Getting Easier
- Detection Has Failed on Some Occasions

The extraordinarily rapid rate of change in the cyber realm, as well as the unique threats that Israel faces, mean that effective detection and early warning are of particular importance. It is thus hardly surprising that Israel has developed highly sophisticated intelligence collection capabilities and that cyber has become the primary means by which it does this, as it has for most advanced states. Cyber has also become a primary basis of Israel's concept of intelligence-based warfare and an important part of the campaign between the wars. It further plays a role for broader strategic purposes, such as the confrontation with Iran.

Israel's detection and attribution capabilities are abetted by the limited number of truly cyber-capable adversaries it faces, its deep familiarity with their capabilities, and the cooperative agreements it has signed with other states. The sheer number of attacks means that Israel cannot attribute them all, but when it has been important, attribution does not appear to have been a significant obstacle for Israel to date, at least at the intelligence level, if not necessarily the requisite diplomatic and legal ones. Further, it is not necessary or useful to expend resources on low level attacks by smaller actors, which reduces the number of attacks Israel needs to assign attribution to.

Stuxnet, Operation Orchard, and other offensive cyber operations reportedly conducted by Israel required exquisite intelligence. Intricate and outstanding

intelligence was also necessary for defensive purposes, as evidenced by the absence of major successful attacks against Israel to date. Nevertheless, Israel's detection capabilities have failed on a number of occasions. To cite just two examples, the attack on the Amital logistics firm was discovered almost by chance and a few years elapsed before discovery of the Hezbollah-affiliated Cedars of Lebanon attack against 250 telecommunications, IT, and infrastructure firms in Israel and around the world.

Finding 7: Cyber Defense Is Possible, but Consistent Defense Is Only Really Possible against Lower-End Attacks

- Israel's Experience Demonstrates That Standalone Cyber Defense Is Only Feasible for Lower-End Attacks
- Effective Defense Is Closely Interrelated to Deterrence, Detection, and Resilience
- Israel Is Considerably Better Defended Today; Few Attacks of National Significance Have Succeeded
- Concerns Persist Regarding the Actual Levels of Civil and Military Cyber Security
- Israel Is Only Now Beginning to Address the Threat of CNI Attacks

Israel's experience demonstrates that standalone cyber defense is only feasible for lower-end threats. For sophisticated threats, defense has proven more effective when combined with deterrence, detection, and resilience, all designed to mitigate the severity of the attack and reduce the need for defensive measures. Deterrence is very difficult to achieve in the cyber realm, and some attacks will get past the very best detection measures, thereby necessitating not only effective defenses but also a resilient capability to bounce back following an attack. Israel has thus empowered critical civil and defense capabilities with in-depth cyber defenses, based on multiple, overlapping, and mutually supportive measures, both passive and active. Israel is considerably better defended today than it was in the past and, importantly, few successful attacks of national significance have taken place.

Nevertheless, considerable concern exists regarding the levels of cyber security actually achieved. The gaps in public and private sector cyber security are self-evident, as evidenced by the string of successful attacks against Israeli firms and hospitals in 2020–2021. There are even question marks regarding the cyber security of critical national infrastructure, which has been the primary focus of Israel's defensive efforts for two decades. The numerous public and private sector organizations that are not defined as critical and thus not directly

defended by the INCD—but that still have important ramifications for national life—are even less well defended. Israel may thus be more advanced in cyber security methodology than in praxis. Concern that the defense establishment's defenses may also not prove sufficient is palpable, despite its far greater awareness of the dangers and the extensive measures it has adopted.

The primary focus of concern is CNA attacks against both the civil and military cyber realms. CNE attacks, by their nature, are particularly difficult to detect and consequently to defend against. Israel has only just begun considering how to defend itself against CNI attacks. CNE and CNI attacks are also conducted by otherwise friendly states, not just by enemy ones, whether for purposes of politico-military or commercial espionage or influence campaigns.

The comparative success of Israel's cyber defenses to date is a crucial achievement, but also a potential source of overconfidence. In the absence of the type of trauma caused by a successful attack of national magnitude—such as Stuxnet caused Iran—many public and private sector organizations have yet to take measures commensurate with the magnitude of the threat, at least as perceived by the INCD and government as a whole. As a result, Israel has suffered repeated small-scale attacks against the public and private sectors and is largely developing its response on the go. The problem is that the "big one" may very well still be coming.

Finding 8: Cyber Is a Key Military Tool and Can Help Defeat the Enemy, but Cannot Do It Alone

- Israel's Experience Demonstrates That Standalone Cyber Defeat Cannot Usually Be Achieved, but Strategic Objectives Can
- The Likelihood of Standalone Cyber Warfare Is Very Low
- Israel Adopted a Cross-Domain and Cumulative Approach
- Israel's Offensive Cyber Thinking Is Highly Ambitious
- Cyber Superiority, Not Defeat, Is the Objective

Israel's experience to date supports the position that adversaries cannot usually be defeated solely by cyber means, much as it has shown that standalone cyber deterrence and defense are rarely feasible. To the extent that cyber defeat is achievable, in the classic sense of either preventing an adversary from continuing to conduct cyber operations or undermining its psychological will to do so, it will usually stem from overall military decision, both cyber and kinetic. In the asymmetric conflicts that Israel is engaged in today, against both state and substate actors, it has yet to achieve decisive military outcomes, whether cyber or otherwise.

A corollary of these findings is that the Israeli experience, as posited by various theorists, demonstrates that the likelihood of standalone cyber warfare is also very low. Conversely, there is nothing in Israel's experience, including attacks on Hamas's cyber headquarters and other capabilities, to indicate that hybrid cyber-kinetic conflicts are likely to be any less violent than the purely kinetic conflicts of the past.

The finding that standalone cyber warfare and defeat are unlikely, should not be misconstrued to mean that Israel's offensive cyber thinking is not highly ambitious, that it does not perceive an important role for standalone cyber operations, or does not seek to achieve widespread systemic effects, especially in wartime. Israel has apparently already put offensive cyber capabilities to effective use for strategic purposes, for example, in the attacks against the Iranian and Syrian nuclear programs. In the former case, Stuxnet was deployed as a standalone weapon and designed to achieve significant effects. Israel may have even hoped it would achieve a decisive military outcome (defeat) regarding the nuclear program. In the Syrian case, cyber was employed as part of a broader kinetic operation. The IDF uses cyber operations both during periods of heightened conflict and in the periods between the major rounds of fighting, to support other capabilities. Indeed, cyber has become integral to IDF war fighting capabilities.

Instead of standalone cyber defeat and much as in the case of cyber deterrence, Israel takes a combined cross-domain and cumulative approach. To this end, it not only seeks to employ the entire range of capabilities available to it but engages cyber adversaries repeatedly over time, in order to impose costs on them and reduce their incentives to continue launching attacks. The ongoing exchange of cyber and kinetic attacks, attributed to Israel and Iran during 2020–2022, is both a manifestation of this approach and an indication of its limitations. Stuxnet is also illustrative of these points. Stuxnet successfully damaged Iran's nuclear program and might have even caused a long-term delay had a programming error not led to its discovery, but would probably not have derailed it entirely. When combined with economic and diplomatic pressure, however, Stuxnet may have created the necessary conditions to force Iran to the negotiating table and when combined with kinetic sabotage operations, formed part of a long-term effort to thwart the Iranian nuclear program.

Instead of cyber defeat, Israel appears to seek cyber superiority. Cyber superiority can be achieved in one of two ways: either by reducing the number and severity of cyber attacks to a level that the state can tolerate and at which it can continue to function effectively or by imposing an intolerable level of disruption or damage on the adversary. In effect, cyber superiority is a function of all four Ds along with resilience: deterrence, to reduce the need to defeat adversaries; detection, to alert the state to those attacks that are not deterred; defense, to

minimize the number of attacks that get through; and resilience, to bounce back rapidly from them. Israel's focus to date, as in the case of cyber defense and for similar reasons, has been primarily on CNA attacks.

Finding 9: Cyber Attacks Appear Less Escalatory Than Kinetic Ones, at Least Under Certain Circumstances

- Israel's Experience Indicates That Cyber Attacks Are Less Escalatory Than Kinetic Ones, but Is Not Conclusive
- Both Israel and Its Adversaries Appear to Believe They Are Less Escalatory
- Israel's Cyber Operations Are Constrained by the Risks of Retaliation and Escalation

It is still too early to conclude definitively whether Israel's experience demonstrates that cyber attacks are more or less escalatory than kinetic ones. The record to date provides mixed evidence, leaning to the latter, and indicates a range. Below a certain, as yet indeterminate level, cyber attacks do appear to be less escalatory; above it, the risks of escalation increase. One thing, however, appears to be abundantly clear. At least as far as Israel's primary adversaries are concerned—Iran, Hezbollah, and Hamas—the cyber realm does provide them with an important additional means by which to wage the conflict against Israel, without incurring a significant risk of retaliation and escalation. Israel is only known to have responded to cyber attacks by cyber means on isolated occasions and to have responded to them kinetically just twice.

Israel, too, appears to consider cyber attacks less escalatory than kinetic ones. Cyber operations are a part of Israel's concept of the covert campaign between the wars and are explicitly designed to be less escalatory. Stuxnet was launched in the belief that this would be the case and Iran did not, in fact, respond directly, either kinetically or by cyber means. Conversely, Iran's decision to develop its own cyber capabilities and the wave of cyber attacks that it launched just two years later, after those capabilities had taken shape, was a direct result of Stuxnet. Moreover, Iran has become one of the more aggressive states in the cyber realm ever since. In this sense, Stuxnet did result in a clear cyber escalation.

In the late 2010s and early 2020s, Israel and Iran apparently engaged in an ongoing exchange of cyber and kinetic blows, which ceased to be covert, even if neither generally took credit and the details remain murky. In practice, neither side appears to have been so concerned about the potential escalatory ramifications that it was deterred from further attacks, and yet both sides ultimately demonstrated restraint. In 2020, Israel reportedly responded to an

Iranian attack on its water system by escalating to an even more severe attack on an Iranian port, to which Iran then responded with further, but clearly limited, attacks on the water system. Most of Iran's attacks throughout the rest of that year were limited to ransomware attacks. Ransomware attacks are certainly disruptive and costly, but not as escalatory as attacks on critical infrastructure, thereby indicating possible Iranian reticence to escalate further. Israel is not known to have responded either to the second round of attacks on the water system or to the ransomware attacks.

Critically, Israel is far more cyber-dependent than its adversaries, and its offensive cyber operations appear to be at least partly constrained by the risks of retaliation and escalation and of a prolonged cycle of cyber attack and counterattack. It is especially wary of attacks against critical national infrastructure and other important civil and military targets. Israel has reportedly conducted numerous kinetic attacks against Iranian and Iranian-affiliated targets in Syria and elsewhere in the region, seemingly with little concern over the escalatory consequences, but it either conducts far fewer cyber attacks or does a far better job of hiding the evidence. It is also possible, of course, that Israel is simply holding its cyber capabilities in reserve, for the outbreak of major hostilities or some other particularly important timing of its choosing.

Overall, the record suggests a picture of escalatory restraint in the cyber realm, at least at certain levels of conflict, although it is not clear if such restraint will continue to hold. The cyber realm is still new, and the rules of the game are not yet clear. Whether these findings substantiate the actors' belief in the less escalatory nature of the cyber realm and contribute significantly to the theoretical debates in this area or simply reflect the limitations of the available information is unknown. In keeping with constructivist thought, if states believe that cyber attacks are less escalatory, they may be more likely to use them, and norms may not develop against their use. This could lead to a proliferation of cyber attacks and contribute to mistakes that lead to unintended escalation.

Finding 10: Cyber Is Neither Inherently Offense nor Defense Dominant and Will Evolve as Capabilities Change

- Israel's Experience Does Not Demonstrate Conclusively Whether Cyber Offense or Defense Has the Upper Hand
- Israel Seeks to Take Cyber to the Enemy but Is Constrained by the Risks of Escalation
- The Relative Weight of Cyber Offense and Defense Will Evolve as Capabilities Change

Israel views the cyber realm as a continually contested space, in which states engage in ongoing contact and friction. Moreover, the cyber realm has provided Israel's adversaries with at least a veneer of anonymity and expectation of impunity, thereby providing an incentive to launch attacks against it. These advantages are further strengthened by the absence of binding international norms or regimes to constrain state behavior in the cyber realm. In this sense, Israel's experience indicates that cyber has been offense dominant.

This finding is further strengthened by Israel's own behavior. In keeping with the IDF's long standing preference for the offense, Israel's military cyber doctrine is based on active defense and transferring the battle to the enemy, rather than waiting to be attacked and merely engaging in defense. Cyber has also allowed Israel to reach targets that would have been difficult to attack using traditional military means, without having to risk soldiers' lives.

Without detracting from Iran's fundamental hostility toward Israel and the potential severity of the threat that it poses in the cyber realm, much of Iran's activity in the cyber realm has clearly been reactive and in that sense defensive. Moreover, Iran and other adversaries have succeeded in conducting only a few attacks of significance against Israel, most of which were against lightly defended public and private sector targets, the proverbial low hanging fruit. This finding strengthens the belief that most Israeli targets of importance are defended at a level beyond all but the most sophisticated attacks and therefore supports the contention held by some theorists that cyber is defense dominant. Further support for this contention is lent by the conclusion that Israel's concerns regarding the dangers of escalation in the cyber realm have served to constrain its offensive behavior, mentioned earlier.

In short, it is premature to judge, based on Israel's experience to date, whether the cyber realm is offense or defense dominant. The conclusion, to the extent that any can be derived, is that the cyber realm is inherently neither, and the relative advantages of cyber offense and defense will evolve, as has been the case with all weapons throughout history, as capabilities and strategies develop over time.

Finding 11: Cyber Strengthens Advanced Actors More Than Weaker Ones

- Cyber Provides Weaker Actors with New Capabilities, but Strengthens Technologically Advanced Actors Even More
- Israel Has Taken Advantage of the Cyber Realm More Successfully Than Less Advanced Rivals

In the debate between those who believe that the cyber realm strengthens weaker actors, by providing them with asymmetric means to offset the greater power of their adversaries, and those who believe that the technological capabilities required to make effective use of the cyber realm strengthen advanced states even more, Israel's experience lends greater credence to the latter.

Israel's adversaries have certainly made growing use of their cyber capabilities, but Israel has applied cyber to far greater economic and military effect. Moreover, Israel makes effective use of some of the same asymmetric advantages that cyber proffers to its adversaries, in addition to concurrent or sequential use of both cyber and kinetic capabilities. It thus enjoys the advantages of both worlds. The bottom line has been a net overall relative gain in military power for Israel over its adversaries.

Finding 12: Investment in Research, Innovation, and Collaboration Is Critical to Cyber Success

- Israel's Unique Cyber Ecosystem Was the Sine Qua Non for Its Emergence as a Global Cyber Power
- The Ecosystem Is Based on an Innovative Culture, High Investment in Cyber R&D and Education, and Incentives for Multinational Tech Firms
- Domestic Constraints Risk Israel's Position as a Leading Cyber Power

Israel's unique cyber ecosystem, based on highly innovative national and strategic cultures, were the sine qua non for its emergence as a leading global cyber power, notwithstanding its otherwise diminutive size. The creative tension generated by a highly heterogeneous immigrant society was further amplified by the creative insecurity stemming from an ongoing state of severe external threat. Both imbued Israeli society with a number of cultural attributes that are particularly suited to the cyber realm, including an extraordinarily nonhierarchical and informal character; strong cultural resistance to rules and established ways of doing things; and an unusual willingness to improvise and take risks.

Israel's investment in R&D, which is among the highest in the world, along with a highly educated and scientifically sophisticated workforce, have been key to its success, further reinforced by extensive incentives designed to attract the major multinational tech firms. Cutting edge academic research has propelled advanced commercial applications. Cyber education programs, from public school through university, have expanded the overall national cyber workforce. All of Israel has essentially become one national cluster, a type of social network that has been found to play a key role in the cyber realm.

Israel's cyber ecosystem remains highly dynamic and continues to grow, but it is maturing, and the number of new startups has slowed appreciably. Government support for cyber R&D has diminished, mostly because sufficient funding is now provided by the capital markets and multinational tech firms, but they will rapidly move elsewhere should the opportunities prove more attractive. A growing challenge from competitors abroad, shortage of highly qualified cyber personnel despite the various programs designed to increase the national pool of cyber talent, severe brain drain in critical areas, and long-term deterioration of the national educational system are the primary impediments to further growth. If Israel does not act to address these issues decisively and in a timely fashion, it stands to lose its leading position in cyber and high-tech generally.

Finding 13: Governments and Defense Establishments Can Be the Primary Drivers of Cyber Innovation

- The Defense Establishment's Contribution to Israel's Cyber Success Cannot Be Overstated
- Military Conscription Has Generated a Cyber Talent Pool Akin to That of a Global Power
- A Symbiotic Relationship Exists between the Defense Establishment and Other Sectors of Israeli Society

The importance of the defense establishment's contribution to Israel's cyber prowess cannot be overstated. Military conscription has provided a uniquely Israeli solution to the need for highly qualified personnel, and one that has, remarkably, generated a national cyber talent pool that is, in absolute numbers not just qualitatively, on the order of a major power's talent pool. The needs of the IDF and intelligence agencies have driven investment in military cyber R&D and spawned numerous private firms and civilian applications. Technologically advanced units of the IDF and intelligence agencies have become incubators and accelerators of cyber startups, and veterans head and staff a large percentage of all cyber firms in Israel. To meet its needs, the IDF has been one of the driving forces behind cyber education, both in the public school system and during military service.

The IDF and intelligence agencies are imbued with the same innovative culture typical of the civil sector, further buttressed by the highly disciplined and focused pursuit of missions typical of defense organizations. A symbiotic relationship exists in Israel between the defense establishment, government, academia, and public and private sectors. Knowledge, capital, and personnel flow from the defense establishment to them and back.

The special attributes of the Israeli cyber ecosystem may not be replicable in precisely the same manner elsewhere, especially in the absence of military conscription and the special civil-military relationship. Nevertheless, the success of Israel's cyber ecosystem offers invaluable insights that other states can adapt to their circumstances and needs.

Finding 14: No One Can Go It Alone—International Cooperation Is Critical in the Cyber Realm

- Cyber Cooperation Has Strengthened Israel's Bilateral Ties and Regional Standing
- International Cooperation Is an Important but Under-Resourced Part of Israel's Cyber Strategy
- There Are Reservations Regarding the Applicability of International Law
- There Is Strong Support for a "Multi-Stakeholder" Approach to the Civil Cyber Realm

International cooperation has been an important component of Israel's cyber strategy, contributing not just to a strengthening of its commercial and military cyber capabilities but also to an improvement in Israel's foreign relations and regional standing. The breakthrough establishment of new ties with a number of Arab states, known as the Abraham Accords, and the expansion of ties with a variety of others were motivated in part by their interest in cyber cooperation. Despite the government's clear recognition of the importance this and of active participation in international cyber discourse, it has not fully availed itself of the opportunities to promote international cooperation, and its efforts do not enjoy sufficient funding, personnel, or central direction.

Cyber cooperation has also been a source of diplomatic friction with various states, primarily over the sales of advanced cyber capabilities to authoritarian regimes. The international backlash has forced Israel to re-examine its cyber export policies and impose greater oversight. Israel has also been less successful in leveraging cyber diplomacy in multilateral forums, where the Palestinian issue weighs heavily.

The international discourse regarding the applicability of international law to the cyber realm presents Israel with difficult dilemmas. On the one hand, Israel supports the principle of a rules-based international order. On the other, bitter experience clearly demonstrates that international norms, regimes, and law are flouted as a matter of course in the Middle East and are thus of questionable applicability to the region. There is also a concern, once again based on extensive experience, that Israel's legitimate right to self-defense will not be recognized by

many states, even if cyber attacks can be attributed directly to the source and the damage it has suffered is significant. Moreover, cyber attacks against Israel are launched by a wide range of state and nonstate actors, meaning that the number of actors to be covered by an international norm, or regime, would be enormous and essentially unenforceable. Maybe most importantly, Israel would presumably be loath to place limitations on its unique cyber capabilities in the name of international norms of dubious effectiveness.

Israel has thus adopted a cautious approach toward the applicability of international law to the cyber realm, emphasizing the need for further experience before informed decisions can be made. Some support has been mooted for adoption of a special and more stringent regional cyber regime, as opposed to a global one. In contrast with Israel's cautious approach in these areas, its support for the open and free, Western, "multi-stakeholder" approach toward the cyber realm, as opposed to the Russian and Chinese emphasis on state sovereignty and control, is staunch and unequivocal.

Israel Specific Conclusions

Conclusion 1: Civil Cyber Security Is the Only Area of National Security in Which Israel Has Adopted a Formal Strategy

- Israel Was among the First States to Formulate a Civil Cyber Strategy
- Civil Cyber Security Is the Only Area of National Security in Which Israel Has Adopted a Formal National Strategy
- Establishing a Single Entity Responsible for All Civil Cyber Affairs Was Key
- The Strategy's Primary Shortcoming Is an Absence of Clearly Defined Objectives

Israel was among the first states to identify the threats and opportunities posed by the cyber realm and to begin adopting the decisions that ultimately evolved into a comprehensive civil cyber strategy. Establishment of a single national entity, the INCD, responsible for all national efforts in the areas of public and private sector cyber security and capacity building, was a key decision.

Inevitably, the strategy has various shortcomings, notably the absence of clearly defined objectives and consequently of a multiyear work plan for achieving them. Promotion of the national cyber ecosystem and of international cyber cooperation are two of the areas in which the absence of clearly defined objectives is most acutely felt. Nevertheless, civil cyber security stands out as

the only area of national security in which Israel has adopted a formal national strategy.

As already indicated in Finding 3, why this came to be is an interesting question worthy of further study. Partly it reflects the fact that the cyber threat was such a new and novel realm that it did not fit neatly into any preexisting strategies and organizational structures. Partly it may reflect the character of the leading individuals involved, including the prime minister, primary drafters of the cabinet decisions, and founding heads of the INCD.

Conclusion 2: Israel's Civil Cyber Response Has Been Effective, but the Resources Allocated Are not Commensurate with the Threat

- Compared to Other Threats and States, Israel's Cyber Response Has Been a Signal Success
- The INCD Has Done a Good, if Imperfect, Job of Fulfilling Its Tasks
- Nevertheless, There Is an Incongruence between the Magnitude of the Threat and the Resources Allocated

Some seven years after the primary cabinet decisions were adopted and the INCD was established, the strategy they embody has provided an impressive overall response to the cyber needs of Israel's public and private sectors. Israel's cyber ecosystem continues to flourish, few severe cyber attacks have successfully taken place, and, in challenging circumstances, the INCD has done an effective, if imperfect, job of fulfilling the tasks assigned to it. No strategy is without its failings and blemishes, however, including the cabinet decisions and 2017 INCD Strategy. We have already indicated the primary failings above.

There is at least some incongruence between the magnitude of the cyber threat that Israel perceives and the resources it has devoted to the INCD and civil cyber security generally. To be sure, this is not a case of resource-poor agencies and programs. The INCD is well funded and staffed, all government agencies today have their own cyber security programs, and the ISA remains deeply involved in civil cyber security. By way of comparison, however, the UK equivalent of the INCD has approximately double its staff. Admittedly, the UK's population is much larger than Israel's, yet the functions that must be fulfilled are quite similar and the threats Israel faces are comparable, if not considerably greater.

Moreover, Israel's investment in cyber is far smaller when compared to another, and in many ways similar asymmetric threat, terrorism. A large part of the IDF's budget, forces, and operations are devoted to counterterrorism, as are the overwhelming part of the ISA's and a significant part of both the Mossad's and

Israel Police. To give another example, the INCD's total staff is similar in size to a single IDF battalion, of which it has dozens. Again, the comparison is decidedly imperfect, but if the threat is as severe as stated—one of the top few Israel faces today, with potentially systemic effects—the investment appears relatively modest.

Less information is publicly available regarding the response by the defense establishment, and our conclusions are therefore more tentative, but it does appear to have taken measures more commensurate with the magnitude of the threat and opportunity. The IDF has established robust cyber units and developed highly sophisticated capabilities, both for offense and defense. The intelligence community is deeply invested in cyber, both in terms of the number of personnel and operations, and cyber has become Israel's primary means of intelligence collection generally.

When viewed from a broad historical perspective, it is hard to think of another area in which Israel has geared up to address an emerging threat, or opportunity, as rapidly and effectively as it has in the cyber realm. Compared to Israel's response to the rocket threat, which really began to emerge in the 1990s, around the same time as the cyber threat, or the terrorist threat, which predates the state's establishment, the response in the cyber realm stands out as a signal success. This is also true when compared to many, maybe most, other states around the world.

Conclusion 3: The IDF Has an Operational Cyber Doctrine, Not a Comprehensive Strategy

- By Design, or by Default, Israel Has Adopted a Policy of Military "Cyber Ambiguity"
- The Civil Strategy and Military Doctrine Are Not Fully Integrated
- It Is Not Known How Cyber Complements Israel's Nuclear Strategy

Unlike the civil cyber realm, in which Israel has developed a coherent national cyber strategy, the IDF has developed an operational cyber doctrine but not a comprehensive military cyber strategy. Although convergences exist between the civil and military approaches, an overall national cyber strategy, integrating both realms, has also yet to be formulated.

In the absence of a fully explicated and openly declared military cyber strategy, Israel's positions on a variety of issues of importance are not publicly known and can only be surmised from its praxis in some cases and general strategic thinking. To illustrate, we do not know the types of conflicts in which Israel believes that cyber weapons might be used (its praxis indicates all); whether it has adopted

a cross-domain and cumulative approach to cyber deterrence and defeat (its praxis demonstrates that it has); whether Israel has adopted a policy of "no first use" of cyber weapons or envisages the possibility of standalone cyber warfare (its praxis indicates that it does not); and how, if at all, Israel's cyber capabilities have been integrated into its broader national strategy, including its purported nuclear capabilities and counter-proliferation policy, the Begin Doctrine. Of far greater significance than the absence of public knowledge regarding these issues is that some have apparently not been addressed on a classified basis either, at least in an in-depth and systematic manner.

Whether by design or by default, Israel appears to have adopted a policy of "cyber ambiguity," regarding attacks both by and often even against it. The policy of cyber ambiguity provides Israel with the freedom of action necessary to protect its interests, signal its intentions and capabilities to its adversaries, and avoid potential escalation and criticism. Ambiguity has certain constructive advantages, but other states have articulated declaratory postures on issues such as those above, without putting their national security at risk.

Conclusion 4: Israel Has Successfully Handled Attacks to Date, but the Threat Is Growing

- Most Attacks to Date Have Been Unsophisticated and the Damage Limited
- Iran's, Hezbollah's, and Hamas's Capabilities Are Improving Steadily
- Russia and China Are Growing Threats, as Are Some Close Allies
- Given Israel's Narrow Security Margins, Even Brief Disruptions Can Be Critical

Israel faces a nearly constant onslaught of cyber attacks, conducted for purposes of disruption, destruction, espionage, and influence. Attacks have targeted virtually every possible type of network. The attackers' motivations have varied, but most have been politically based and a reflection of the broader Arab-Israeli conflict. The barrage of attacks is ongoing, but spikes during periods of both heightened military tension and, perhaps counterintuitively, diplomatic activity.

Most of the attacks to date have been relatively unsophisticated, or aimed at poorly defended targets, and Israel has usually succeeded in preventing significant damage. The attacks have, however, clearly demonstrated the potential for significant disruption and damage. Given Israel's narrow security margins, even brief disruptions of critical infrastructure systems, let alone military ones, could have significant ramifications for the conduct of military operations and even the outcome of conflicts. The potential for a severe impact on Israel's international standing was clearly demonstrated, for example, by the attacks on the

Eurovision song contest held in Israel and against Ben-Gurion airport, prior to the arrival of global leaders for a commemoration of the liberation of Auschwitz, in 2019 and 2020 respectively.

The mixed CNE, CNI, and cyber crime attacks against Israeli insurance and logistics firms in 2020–2021 may have provided Israel's adversaries with intelligence of considerable importance. North Korea may have succeeded in collecting important information regarding Israel's defense industries and presumably passed it on to Iran. Iranian cyber information operations briefly succeeded in causing nuclear tensions with Pakistan, on one occasion, and in causing concern in Israel following fake reports that the Dimona nuclear reactor had been hit by rocket fire, on another.

The actual sophistication of Iran's cyber capabilities remains a subject of dispute, but there is no doubt that they have advanced significantly and are continually improving. The same is true of Hamas's cyber capabilities and presumably Hezbollah's, too, even if this is not borne out by the publicly available data. The ability of Israel's adversaries to wage effective cyber warfare is unknown. To date, they have focused primarily on less critical and thus less well defended targets, whether due to lack of capability or because they are withholding their advanced capabilities for the right moment.

Global powers, such as Russia and China, are sources of growing concern for Israel in the cyber realm. Close allies, including the United States and UK are too. The apparently still limited capabilities of Arab states, hostile and otherwise friendly, will undoubtedly also improve in the future.

Conclusion 5: The IDF Cyber Force Structure Does Not Maximize Israel's Potential

- Cyber Has Become an Important Fourth Dimension of IDF Operations
- The IDF Has Not Established Functional Commands to Address Other Asymmetric Threats Either
- A Decision on IDF Cyber Force Structure Has Been Delayed for Too Long

For the IDF, cyber has become an important fourth dimension of military operations, alongside the traditional dimensions of ground, sea, and air operations. The IDF has worked assiduously to develop its power in the cyber realm, views it as an area in which it holds the advantage, and, as evidenced by the variety of cyber attacks attributed to it, has used cyber capabilities to promote and defend Israel's interests on a number of important occasions. Stuxnet, Operation Orchard, and the attack on the port at Bandar Abbas stand out in particular as offensive cyber operations and demonstrate how cyber has enabled Israel to

achieve what would have otherwise been difficult, possibly even unattainable, military objectives.

The optimal cyber force structure, whether under a unified cyber command or some other model, is a highly complex issue that has bedeviled the IDF for a decade. There continue to be important considerations on all sides of the issue (see Chapter 10). Notably, the IDF has not established specific functional commands to address other asymmetric threats either. Operational counterterrorism and counter proliferation capabilities, for example, are dispersed through a variety of different functional and regional commands. Conversely, the Air Force and Navy constitute unified functional and inter-regional commands designed to address the entire range of threats that Israel faces: asymmetric, conventional, and nonconventional. Overall IDF strategic planning to address these threats is now divided between three General Staff branches, the long-standing Operations and Planning Branches and a recent spinoff from the latter, the Iran and Strategic Affairs Branch. The failure to resolve the issue is a severe failing that does not maximize Israel's cyber potential.

Conclusion 6: The United States Is Israel's Primary Partner in the Cyber Realm, as in All Others

- There Is Strong Support for Expanded Civil and Military Cyber Ties with the United States
- There Is Concern Not to Expose Israel's Unique Capabilities and Limit Its Freedom of Action
- Israel's Efforts to Assuage the United States Over Cyber Ties with China, but Maintain Relations with China, Have Fully Placated Neither

The United States, with whom Israel engages in extensive cyber cooperation at both the civil and military levels, is its primary partner in the cyber realm, as in all others. Senior Israeli decision-makers express a strong desire for a further expansion of cyber cooperation with the United States, in both realms. In contrast with almost all other spheres of bilateral military cooperation, however, Israel's cyber capabilities are essentially all homegrown and highly advanced. Israeli thinking is thus informed by a deep concern that the state neither risk exposing its unique military capabilities nor constrain its freedom of independent action in the cyber realm. Considerations such as these have long characterized Israel's thinking in all areas of military cooperation with foreign nations, even the United States, and are an important component of the emphasis that Israel's strategic culture places on self-reliance and autonomy. These considerations are particularly pronounced in the cyber realm, however, where Israel's domestic

capabilities provide unique opportunities for action, unfettered by the need to gain the approval of and coordinate with others.

Sales of advanced cyber capabilities to authoritarian regimes in the Middle East and around the world, especially to China, and investments by the latter in Israel's cyber ecosystem, have been a source of bilateral friction with the United States, Israel's foremost strategic ally. Israel has attempted to address US demands that it cease or at least curb cyber cooperation with China, while also trying to minimize the blow to its ties with China, a leading commercial partner and actor of growing importance in the Middle East. In practice, these attempts have succeeded in fully placating neither and failed to prevent a significant downturn in economic ties with China.

Conclusion 7: Cyber Has Strengthened Israel's Overall National Power and Partially Upended the Regional Balance of Power

- Israel Has Leveraged Cyber to Strengthen Its National Power and Strategic Posture
- Cyber Capabilities Have Partially Upended the Regional Balance of Power
- CNI Operations Provide a Nonviolent Means of Constraining Israel's Freedom of Action and Undermining Its Standing

Cyber has at least partially upended the traditional balance of power in the Middle East, as it has at the global level, providing Israel with critical advantages over its adversaries. None of the other Middle Eastern states have digital economies and cyber ecosystems as advanced as Israel's, nor have they applied cyber technologies for military purposes to the extent that it has.

Cyber contributed significantly to the socioeconomic and political turmoil that has continued to erupt in the Middle East ever since the Arab Spring of 2011 and may have contributed both to its precursor in Iran[‡] and to the subsequent outbreaks of unrest there. For reasons that go far beyond cyber, but are greatly abetted by it, this regional turmoil is likely to continue for years and even decades, with significant ramifications for Israel's security. To the extent that Israel's adversaries are militarily weakened by it, and in some ways even economically, the impact on its national security will be positive. Conversely, if their internal stability and national cohesion continue to unravel and violence spills

[‡] The mass demonstrations following the 2009 presidential elections in Iran are considered by some scholars to have been an early manifestation of the regional disturbances subsequently dubbed the Arab Spring.

over the border, the impact on Israel will be highly deleterious. The same holds true if weakened regimes, fighting for their survival, try to deflect domestic attention from their failings by means of conflict with Israel.

Cyber has had an important impact on Israel's regional and international standing. Israel successfully leveraged cyber as a means of establishing and strengthening ties with a variety of states around the world and now engages in cyber cooperation with nearly 100 states. Israel's cyber capabilities were an important reason behind the willingness of the UAE, Bahrain, and Morocco to normalize relations in 2020, the expanding informal relationships with Saudi Arabia and other Arab states, and their interest in cooperating with Israel against Iran. Cyber has also been an important component of improved ties with countries of critical importance for Israel, such as the UK, India, and China. It has, however, placed Israel between China and the United States, forcing it to take sides in a no-win situation.

Cyber information operations have provided Israel's adversaries with important new means of creating international pressure on Israel to halt, or curtail, military operations before it can achieve its objectives. As such, they have had a significantly adverse impact on its ability to effectively wage war and on its international standing. Cyber information operations have also provided Israel's adversaries with a variety of effective platforms for reaching vast numbers of people around the world, directly, instantly, and at minimal cost, as part of their ongoing effort to delegitimize Israel and isolate it diplomatically. Domestically, cyber information operations are not known to have disrupted important political and governmental processes in Israel to date, nor caused significant social discord. The number of such attacks is increasing, however, and concern is growing.

Israel's offensive and defensive cyber capabilities are considered to be highly advanced and have become important components of its military might, as have its cyber-based intelligence capabilities. Israel's ability to conduct cyber information operations for military purposes is less well known, but there are reasons to believe that it, too, may be sophisticated. In practice, cyber has become such an integral part of operations conducted by the IDF and the intelligence agencies, for defensive and offensive purposes or even just to conduct day-to-day operations, that they could hardly function without them.

In a world increasingly averse to physical and especially lethal damage and in which Israel is repeatedly excoriated for allegedly disproportionate uses of force, cyber provides a means of achieving at least some military objectives without loss of life and property and with reduced risks of retaliation and escalation. Stuxnet still stands out for the new and, at the time, even revolutionary means it provided Israel's leaders to achieve strategic objectives that would have required military force in the past. Indeed, Stuxnet may have been a harbinger of a new

era of cyber conflict, with important ramifications for the future of diplomacy, espionage, and warfare, not just for Israel but for the world as a whole. Additional attacks attributed to Israel since then have further reinforced this conclusion, if less dramatically.

Israel's adversaries have also come to appreciate the importance of cyber operations as a nonviolent means of achieving military objectives. This has been evidenced by a variety of cyber attacks, including the hacking by Hamas of unencrypted live feed from road cameras to improve rocket targeting; attacks against the IDF's civilian gas and food suppliers, whose activities can provide important indications of impending military operations; and attacks on commercial logistics firms that could have disrupted Israel's weapons exports and commercial air and maritime cargo traffic.

Israel's vibrant cyber ecosystem constitutes a significant portion of its GDP today and a primary source of economic growth. The Israeli cyber ecosystem is in many ways unparalleled, producing world-class cyber talent, not just in quality but also in absolute numbers that are on a par with major powers. Moreover, the cyber ecosystem is a primary source of military might, generating both unique military solutions that are critical for Israel's security and much of the monetary resources needed to sustain the defense burden. Conversely, Israel's greater cyber dependency, both civil and military, compared to its adversaries, is a major vulnerability, providing those adversaries with an entire array of new opportunities to cause it significant harm.

As is almost inevitable, the picture outlined here is mixed. Overall, however, cyber has had a significant impact on Israel's state power, affecting its strategic environment, military might, foreign relations, and economic prowess. Based on the findings and conclusions presented in this chapter, as well as the previous background chapters, we can now turn to our final and most demanding task: recommendations for a comprehensive civil and military Israeli national cyber strategy.

12

A Comprehensive National Cyber Strategy

Cyber has evolved into the ultimate weapon, the equivalent of a silent nuclear weapon. No armies are involved . . . but the new threat can simply take countries apart.

Tamir Pardo, former head of the Mossad

In the civil (public and private) cyber realm Israel has formulated a coherent and well thought out strategy, as adopted in the relevant cabinet decisions between 2002 and 2015[*] and encapsulated in the 2017 INCD Strategy. As with any strategy, there is room for criticism, and since it draws on cabinet decisions made during that period, long ago in cyber terms, some updating is required. Nevertheless, the basic thinking and concepts behind the strategy remain sound and fundamental change is not warranted. Some of the recommendations presented in this chapter regarding the civil cyber strategy are thus designed to highlight important areas of continuity and draw attention to those that require further attention, rather than suggest the need for major new departures. Other areas are already well explicated and do not require further mention here.

In the national security areas of foreign and defense policy, in contrast, Israel has not formulated a coherent cyber strategy, whether public or apparently classified, and by default this is not integrated it into an overall national security strategy. No official policy statements,[†] or other works of significance, academic or otherwise, have addressed these issues either, and it is in this heretofore uncharted area that the strategy recommended here may make its greatest contribution. In the absence of an existing body of work to serve as a reference point

[*] Decisions B/84 from 2002, 3611 from 2011, and 2443 and 2444 from 2015.

[†] The IDF Strategy (2015 and 2018) is an important exception to the overall absence of formal strategic documents, but its meagre references to cyber are too limited to provide any insights of significance regarding Israel's military cyber strategy.

Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press.
 DOI: 10.1093/oso/9780197677711.003.0013

even to begin from, the recommendations in this chapter draw on all of the preceding chapters, including the theoretical quandaries, international experience in the cyber realm, the few public pronouncements and observable Israeli actions presented in Chapter 10, and especially the conclusions in Chapter 11. We further extrapolate from the strategies formulated by other leading cyber actors and our overall knowledge of Israel's national security needs and strategy.

A proposal for a national strategy, in any field, presents a number of potential considerations and pitfalls. First, strategies are relevant to a given time frame and set of assumptions. The rate of change in the cyber realm is extraordinary and is further amplified in Israel's case by the continually and dramatically changing Middle Eastern environment. In these circumstances, it would be foolhardy to aspire to a strategy relevant to much more than a few years. Conversely, a strategy that cannot withstand the test of time can hardly be considered to be one. We, therefore, suggest that a strategy for approximately five years, with periodic midcourse assessments and recalibration, is appropriate to the exigencies of both the civil and national security cyber realms in Israel.

A second consideration is that the proposed strategy constitutes a broad set of principles designed to serve as guidelines for future planning and decision-making. It is not, and does not purport to be, a detailed blueprint for action in all future scenarios. Formal strategies are designed to leverage the intellectual rigor that goes into their formulation in order to better refine objectives, priorities, and the options for achieving them and thereby enrich decision makers' thinking at the appropriate time. The unique, still relatively novel and seemingly opaque character of the cyber realm lends particular importance to the formulation of coherent and comprehensive strategies for addressing it.

A third consideration is political viability. If a strategy is not politically viable, it may still be of theoretical interest, but does not constitute the basis for real-world policymaking. We believe that the strategy presented here is not politically divisive and should be acceptable to all Israeli governments, regardless of political orientation. This is not to suggest that every recommendation will be accepted but that the debate should be primarily substantive in nature, not partisan.

A fourth consideration is that some of the recommendations are knowingly unoriginal, having been proposed by others in the past. The challenges that Israel and other states face in the cyber realm are familiar to those well versed in its vagaries; various experts have already weighed in, and we are fortunate to be able to draw on their work. It is the integration of the existing wisdom, based on a systematic analysis of Israel's circumstances and needs, together with our own original contributions, that make these recommendations the first effort to present a comprehensive Israeli national cyber strategy.

Finally, some of the necessary information is unavailable, whether because it is classified or for other reasons. This constraint is a fact of life for all researchers and is particularly true of military affairs. We trust that the recommendations will not be found overly wanting.

The chapter begins with a definition of Israel's overall national security objectives, as the basis for proposed objectives in the civil and national security cyber realms. The recommended cyber strategy itself is divided into six conceptual pillars:

1. Strategy, doctrine, and resources
2. Governance and command and control
3. National capacity building
4. The 4Ds: Detect, Deter, Defend, Defeat (Superiority)
5. Aggregate robustness and systemic resilience
6. International cyber cooperation, influence, and diplomacy.

The recommendations are prefaced by a brief background, summarizing some of the salient points from the previous chapters, as a means of focusing the reader's attention on the issues to be considered. We begin with a brief recap of Israel's civil cyber strategy, a definition of its objectives in the national security area generally and cyber realm specifically, and a ranking of the institutions to be defended.

National Security and Cyber Objectives

The civil strategy embodied in the cabinet decisions and subsequent INCD National Cyber Security Strategy was based on four key elements: *national capacity building* through programs designed to promote cyber education, R&D, human resource development, entrepreneurship, and technological innovation; *aggregate robustness and systemic resilience*, to strengthen the public and private sectors' ability to repel and contain cyber attacks, continue functioning while under attack, mitigate damage from successful attacks, and facilitate a rapid return to the antecedent level of functioning; a *defensive strategy* in which the INCD was given lead authority for the prevention, containment, and mitigation of threats to the public and private sectors, especially critical infrastructure and other vital systems; and *international cooperation* with states around the world.

Impressive as the strategy was, it did have a number of flaws. Of these, for reasons explained in Chapter 7, the most important was the absence of a clear statement of Israel's national cyber objectives, whether in the cabinet decisions, or more surprisingly, the INCD Strategy.

Vital national security objectives refer to a core set of fundamental and essentially immutable interests that are independent of—and transcend—the specific threats, opportunities, and governments in office at any given time.[1] In this context, Israel's vital national security objectives are to:

- Ensure Israel's existence, territorial integrity,[‡] and the security of its citizens.
- Preserve Israel's character as the democratic nation state of the Jewish people and as its national home.
- Achieve and maintain peace with Israel's neighbors.
- Promote the socioeconomic well-being, fundamental national consensus,[§] and resilience of Israeli society.[2]
- Preserve the "special relationship" and de facto alliance with the United States. The relationship with the United States—in reality a means of achieving Israel's objectives—is of such overriding importance that it, too, more arguably, may be considered a vital objective in its own right.

In addition, Israel has a variety of lesser, though still supremely important national security objectives, some ongoing, others that change with circumstance. Current examples include preventing Iran from acquiring nuclear weapons and rolling back its influence in the region, especially in Syria and Lebanon, preventing Hezbollah and Hamas rocket attacks and other forms of terrorism, defeating international delegitimization efforts, expanding new opportunities for dialogue and cooperation with Sunni states, and more.

Drawing on these vital and other national security objectives, we propose the following definition of Israel's objectives in the *civil* cyber realm, in descending order of importance. There are additional objectives, these are the ones of paramount importance.

- Ensure the ongoing vitality of Israeli democracy, including the free flow of ideas and data, freedom of expression, and integrity of the electoral system.[3]
- Ensure the ongoing functional continuity of Israel's vital governmental institutions, critical national infrastructure, and other essential systems.[4]
- Prevent or at least minimize cyber disruptions to the functional continuity and vitality of the public and private sectors.

[‡] Pending final resolution of Israel's borders, territorial integrity refers to all areas under Israeli control.

[§] For our purposes, the fundamental national consensus refers to the vital national security objectives stated here and the supremely important, but lesser ones, presented in the following paragraph.

- Promote Israel's cyber ecosystem as a major engine of national economic growth.
- Preserve Israel's technological leadership and standing as one of the world's leading cyber powers.[5]

On the same basis, we further propose the following definition of Israel's objectives in the *national security* cyber realm, in descending order of importance.[6] Once again, these are the objectives of paramount importance.

- Ensure the integrity of the national decision-making processes and ability of Israel's leaders to make decisions without cyber disruption.[7]
- Maintain offensive and intelligence cyber superiority over all regional adversaries, but only effective defense against cyber attacks by leading global powers.
- Ensure the ability of the IDF and defense establishment to achieve their missions (kinetic, cyber, and otherwise) in a contested and disrupted cyber environment, ranging from "gray zones" below the threshold of armed conflict to war.
- Defend Israel's military capabilities, including strategic ones, from cyber attack and support the defense of critical national infrastructure and other vital civil systems, as needed.
- Counter enemy cyber information campaigns, especially during military crises.
- Strengthen Israel's foreign relations and international standing.

The following institutions and systems, to be defended by the state, are ranked by descending order of importance. Significantly, only the first category falls within the sole purview of the defense establishment, most of the other systems are defended by the INCD and other civil agencies.

- Critical national security agencies—including the IDF, intelligence agencies, INCD, and more. These are *not* the intrinsically most important institutions and systems, but their functional continuity is a sine qua non for the continuity of the others.
- The executive and legislative branches of government—including the cabinet, Knesset, Electoral Commission, and critical parts of the judiciary (e.g., Supreme Court).
- Critical national infrastructure, such as energy, water, transportation, and communications.

- Essential governmental and commercial systems, for example, Ministries of Defense and Foreign Affairs, NSS, defense industries, police, health, education, and welfare; population, property, and land registries; local government; as well as financial, trade, and major industrial systems.
- Public and private sector organizations and institutions.

The Six Pillars of a National Cyber Strategy

Pillar 1—Strategy, Doctrine, and Resources

Recommendation 1: Update the Existing Civil Cyber Strategy, Adopt Multi-Year Work Plan

The existing public and private sector cyber strategy is based on cabinet decisions adopted between 2011 and 2015, while the new Cyber Law has essentially remained in abeyance since it was first proposed in 2018. Much has changed in the interim. Areas requiring consideration include, but are not limited to, the regulatory system, cyber ecosystem, systemic resilience, and international cooperation, which is only mentioned in passing in the existing strategy. As noted in Chapter 11, one of the strategy's primary flaws is the lack of clearly defined national objectives in the cyber realm.

- 1.1 Update the civil cyber strategy, with a clear definition of the objectives to be achieved.
  - 1.11 Adopt a multi-year work plan, with benchmarks, to implement the updated strategy.
    - A clear definition of the objectives is the heart of any strategy, cyber or otherwise.
    - In the absence of clearly defined objectives and benchmarks, it is hard to assess whether the INCD and other agencies are performing effectively and to hold them accountable.[8]
- 1.2 Involve primary stakeholders and the public in an iterative process, calling for comments on drafts of the updated strategy, much as was done with the proposed Cyber Law.

Recommendation 2: Formulate Military Cyber Strategy, Integrate into National Security Strategy

The IDF has formulated an operational cyber doctrine, not an overall military cyber strategy. The 2015 and 2018 IDF Strategies state that Israel will conduct

cyber attacks in "support" of other defensive and offensive operations and that the ability to do so, without having to assume responsibility, makes them an important part of the campaign between the wars (MABAM). The current state of thinking in the IDF does not maximize Israel's cyber capabilities and their potential integration with other sources of national power.

- **2**.1 Formulate a comprehensive military cyber strategy.
- **2**.2 Integrate civil and military cyber capabilities into the other elements of Israel's national security strategy. Cyber capabilities are not and not should not be viewed as a standalone category.

Recommendation 3: Ensure Resources Are Appropriate to the Threats and Opportunities

Cyber is both one of the top threats Israel that faces today and a primary engine of economic growth. Chapter 11 presents a number of reasons to question whether the resources Israel allocates to its civil cyber strategy are commensurate with the magnitude of either the threat or the opportunities (socioeconomic, diplomatic, and defense). To cite just one example, the UK equivalent of the INCD is approximately double the size. Even accounting for the difference in national size, the functions to be filled are similar, while the challenges Israel faces are at least as severe.

- 3.1 Ensure that the INCD and other agencies with an important role in the cyber realm, for example, the ISA and Israel Investment Authority, have resources (budgets, personnel, technology) commensurate both with the magnitude of the threat and of the opportunities.
  - Current limitations, budgetary and otherwise, on the INCD's ability to provide the necessary defensive packages, cannot be allowed to determine which organizations are included on the lists of Critical National Infrastructure and other vital entities and the necessary resources must be allocated accordingly. See also Recommendation 4.3.
  - The need to review INCD resources also reflects the expanded role envisaged for it in this strategy in national capacity building, regulatory enforcement, international cooperation, and more.
- 3.2 Build cyber security costs into all future budgets for existing and especially new governmental computer systems and networks.

Pillar 2—Governance and Command and Control

Recommendation 4: Promote Rapid Passage of the New Cyber Law

Not all national security agencies in Israel exist today by statute, but increasingly they do, and this is the desirable end state.** Cyber is still a relatively new and evolving realm, poorly understood by many; it is thus particularly important to enshrine the status of the INCD and regulatory system in statute. Knesset legislation is the highest form of public approbation.[9]

- **4**.1 Promote rapid passage by the Knesset of the 2018 draft Cyber Law, as amended.
  - Most of the concerns raised by government agencies and public interest groups have been addressed in the amended version. Remaining concerns should be rectified over time and should not constitute an obstacle to legislation.
- 4.2 Adopt a statutory definition of critical infrastructure systems and expand the Critical National Infrastructure List accordingly. Conduct periodic reviews of the entities included on the list.

Recommendation 5: Maintain INCD Centrality as Lead Agency, Under Prime Minister

Early recognition that the challenges presented by the cyber realm were the collective responsibility of the governmental, military, public, and private sectors, and that none of them could succeed alone, was critical to Israel's success. Designation of the INCD as the lead agency responsible for governmental, public, and private sector cyber policy, security, and capacity building was similarly critical. Although not without problems, the INCD has proven successful to date in carrying out its overall organizational mission.

- 5.1 Maintain the INCD as the lead agency responsible for governmental, public, and private sector cyber policy, security, and capacity building.
- 5.2 Maintain direct INCD subordination to the premier, thereby providing for ready access and ongoing bureaucratic clout, much as with the Mossad, ISA, and Atomic Energy Committee.
  - The cyber realm may, in the future, mature sufficiently for the INCD to come under a separate ministry. For the meantime, however, its unique role as a

** The IDF, ISA, and NSS exist in statute, the Mossad, Ministry of Foreign Affairs, and others do not.

substrate that undergirds all aspects of modern life warrants its direct subordination to the premier.

- 5.3 Maintain premier's involvement and leadership in the cyber realm.
  - While much of the necessary work has been completed, premier level involvement has been critical to Israel's success in the cyber realm and will help ensure that it continues to receive the attention warranted.

Recommendation 6: Optimize IDF Cyber Force Structure

Seven years (at the time of this writing) after the IDF decided to establish a unified cyber command—and then suspended the decision—nothing has happened, and the time has come to resolve the issue. There continue to be important considerations on all sides of the issue (Chapter 10). Notably, the IDF has also not established specific commands to address other asymmetric threats. Counterterrorism capabilities, for example, are dispersed through a number of functional and regional commands. Conversely, the IAF and Israel Navy constitute combined functional and inter-regional commands, designed to address the entire range of threats that Israel faces, asymmetric, conventional, and nonconventional.

At present, intelligence collection and offensive cyber operations remain the responsibility of MI (Unit 8200); defensive operations are under the C4I and Cyber Defense Branch; and partial coordination and direction is provided by the Operations Branch. This force structure does not optimize IDF cyber capabilities and their integration into an overall military strategy.

- 6.1 Resolve the issue of the IDF cyber force structure, one way or the other. The choice today is between a number of models, of which some of the primary ones are:
  - 6.11 Perpetuation of the current situation.
  - 6.12 Establishment of a unified General Staff Cyber Command, responsible for all offensive and defensive IDF cyber capabilities.[10] [††]
  - 6.13 A hybrid model, for example, maintaining the existing separation between the IDF's offensive and defensive cyber units but establishing separate inter-agency task forces for cyber offense and defense, comprised

[††] There are three primary variations on the unified cyber command model:

- Transfer of Unit 8200 and the Cyber Defense Brigade (which is part of the C4I and Cyber Defense Branch), in their entirety, to the new command. This option has the advantage of fully centralizing IDF cyber operations but would essentially eviscerate MI and likely weaken

of the IDF (Unit 8200 and the C4I Branch), Mossad, ISA, MoD, INCD, and other agencies as needed.[11]

Recommendation 7: Establish Effective Inter-Agency Cyber Coordinating Mechanism; Streamline Division of Authority between Agencies

No formal mechanism exists today, below the cabinet, for determining and coordinating military and intelligence cyber priorities, integrating the civil and military cyber strategies, and assigning organizational responsibility for carrying them out. The coordinating mechanism led by ISA (Chapter 10) is an informal arrangement designed to overcome the void created by the failure of the statutory inter-agency committee, provided for in Cabinet Decision 2443, to convene on a regular basis and fulfill its legally mandated role. Moreover, a gray area exists regarding the division of authority between the INCD and various defense bodies, especially in wartime.

- 7.1 Revitalize the existing inter-agency committee, or establish a new one, to better coordinate and integrate cyber policy, including recommendations to the cabinet regarding peacetime and wartime priorities.
- 7.2 Adopt a multi-year work plan and budget for each agency, with benchmarks, to implement the integrated strategy.
- 7.3 Further streamline the division of authority between the INCD, IDF, ISA, and other defense agencies.

  - A number of areas require further explication, including: the final division between the INCD and ISA, which repeated cabinet decisions have failed to delineate; the IDF's role in containing and remediating extreme attacks

intelligence collection. It would also raise strong bureaucratic opposition from MI and likely the C4I and Cyber Defense Branch.

- Transfer of just some critical cyber components from Unit 8200 to the unified command, along with the entire Cyber Defense Brigade. The blow to intelligence collection and MI, as an organization, would be far more limited, and IDF cyber operations would be significantly centralized. Disagreement would likely still arise, however, regarding the specific components to be transferred and this is a sub-optimal arrangement.
- Unit 8200 and the Cyber Defense Brigade remain within their respective organizational homes (MI and the C4I and Cyber Defense Branch) but are directly linked to the new cyber command and provide it with real-time support, much as they do today with the IAF and navy. This option has the benefit of creating a centralized cyber command but does not maximize its potential.

on the public and private sectors during peace time; and the IDF's overall responsibility for the national cyber realm in wartime.

Recommendation 8: Adopt Semi-Annual Set of Cyber Guidelines; Provide Commanders with Detailed Guidance on Cyber Operations

Unlike most other weapons, sophisticated cyber weapons are not fungible, that is, they cannot be used against a broad variety of targets but only those they were specifically designed to attack. Moreover, the ability to modify cyber weapons or change targets once an operation has begun (adaptive planning) is limited. Cyber operations are instantaneous, but require lengthy preparatory processes, far exceeding the time typically required for kinetic operations. Given these limitations, as well as the need for instant and even autonomous responses, highly detailed rules of engagement (ROEs) are particularly important. ROEs delineate the circumstances in which commanders are authorized to conduct operations on their own recognizance, the nature of the response, and the limitations thereon.[12]

The existing approval process for cyber operations is similar to that for kinetic operations. Standard operating procedures set the parameters for defensive operations and for cyber intelligence collection, without the need for further approval. Offensive and information operations, conversely, require the approval of the chief of staff, defense minister, and even prime minister and are usually dealt with on an ad hoc basis.

- 8.1 Adopt a semi-annual set of guidelines, approved by the defense minister and premier, setting out the types of targets and weapons to be used, priorities, and levels of command authorized to approve cyber operations.
  - Doing so would complement a long-standing recommendation that the defense minister and premier approve an annual strategic guidance document for the IDF and intelligence services, setting out the policy objectives to be achieved and consequent priorities for intelligence collection and operations. See Recommendation 15.2.
- 8.2 Identify, vet, and approve cyber targets and operations in much the same way as kinetic ones. Incorporate offensive cyber operations and active defenses into the defense minister's and premier's standing operations approval processes.
- 8.3 Provide commanders with detailed guidance on the objectives of cyber operations and planning priorities,[13] over and above that customarily provided in kinetic operations.
- 8.4 Authorize senior military and intelligence officials (e.g., chief of staff, regional commanders, and heads of the cyber units, such as Unit 8200) to approve predetermined types of offensive cyber operations without further

approval and to take all passive defense measures, within their own systems and networks, on their own recognizance.

Recommendation 9: Strengthen the INCD's Public Profile and Presence

Private sector entities do not yet sufficiently view the INCD as their first and primary source of cyber security expertise and assistance, nor appreciate the benefits of regulatory compliance and cooperation with it. This public image undermines the INCD's ability to effectively fulfill the roles assigned to it.

- 9.1 Conduct outreach programs to strengthen the INCD's public profile and presence in the field and promote greater awareness of its role and appreciation of its importance for the specific individual or organizational user and for Israel's cyber realm as a whole.
- 9.2 Strengthen and expand procedures for promoting shared situational awareness between the INCD and public and private sector entities.[14]
  - 9.21 Ensure sufficient and timely information exchanges, including maximal distribution of unclassified and declassified cyber threat information, malware forensics, and network data.[15]
  - 9.22 Establish channels for information exchanges tailored to the needs of specific sectors, drawing on the cyber expertise of the different government agencies and CERT-IL sectoral SOCs.[16]

Recommendation 10: Strengthen Cyber Export Regulations and Oversight Mechanisms

Cyber exports are critical sources of foreign income, including the financing necessary for domestic military R&D and procurement. Offensive cyber exports to unsavory regimes, much like those of conventional weapons made by states around the world, require a difficult balance between necessity, both economic and strategic, and moral considerations. There is no simple answer. Nevertheless, the questionable exports of just a few Israeli cyber firms have drawn highly adverse international coverage and caused disproportionate harm to Israel's international standing.

- 10.1 Strengthen export regulations and oversight mechanisms.
  - 10.11 Establish inter-agency oversight committee, under the National Security Staff, to approve cyber export policy and major or sensitive sales. Provide the Ministry of Foreign Affairs with the prerogative to reject sales, with disputes to be resolved by the inter-agency committee and, as necessary, the premier.

- A situation in which the agency with the greatest interest in weapons sales bears primary responsibility for policy and oversight is untenable. The MoD cannot police itself, as has long been demonstrated by conventional weapons sales to China and other states.

Pillar 3—National Capacity Building

Recommendation 11: Adopt a National Science Strategy; Adopt Multiyear Cyber Capacity Building Plan

Israel is a top global cyber power and continues to score impressively on most, but not all, indices of overall high tech and cyber prowess. A number of trends are of concern. Israel's educational system continues to suffer from a long-term deterioration in the quality of its outputs. The vast resources required to develop highly sophisticated cyber capabilities often exceed the budgetary and technological capabilities of states, certainly of Israel's size, and are often only available to the multinational tech firms. These firms may leave Israel at any time, should more attractive opportunities arise. Financing for cyber R&D comes overwhelmingly from the multinational tech firms, rather than the government, whose investment in R&D, especially academic, is now low compared to the OECD average. As a result of these factors, the cyber industry's overall rate of growth has slowed.

- 11.1 Reverse the deterioration in Israel's educational system.
  - This recommendation exceeds the scope of this book but is critical to Israel's cyber and high tech future.
- 11.2 Adopt a national science strategy to foster and protect Israel's competitive advantages and achieve strategic advantage.[17]
    - 11.21 Identify emerging technologies of importance to Israel, whether they represent threats or opportunities.[‡‡]
    - 11.22 Maintain overall existing hands-off approach, encouraging technological development in all areas, but identify and incentivize a number of priorities.
    - 11.23 Adopt and implement the recommendations of the already extant public task forces in the areas of AI, big data, and quantum computing. Integrate their recommendations with cyber policy.
- 11.3 Adopt a multi-year national cyber capacity building plan, including:

[‡‡] In 2022 a report by the Council on Civil R&D recommended that Israel prioritize five new areas, in addition to the existing emphasis on artificial intelligence and quantum computing. The five new areas were: bio convergence (which combines biology, engineering and medicine), food tech, renewable energy and energy storage, civil space applications, and the sea as a national resource, including for purposes of aqua agriculture.

11.31 Clear objectives and benchmarks for development of the cyber ecosystem.

11.32 Increased governmental support for academic cyber R&D, to maintain Israel's scientific lead, and assess the need for heightened governmental investment in commercial cyber R&D, to counteract over-dependence on foreign investors and multinational firms.

Recommendation 12: Enlarge the National Pool of Cyber Personnel

Closely related to the problems identified in the background to Recommendation 11, Israel suffers from a severe brain drain of PhDs in critical areas, and the shortage of highly trained cyber personnel has become a critical bottleneck

- 12.1 Maintain compulsory military service, at least at approximately the current length, as a critical component of Israel's military cyber power and overall high tech prowess.
  - Much like Recommendation 11.1, the issue of compulsory military service exceeds the scope of this book, and critical considerations that go beyond the cyber issue must be taken into account. As seen in Chapter 8, however, compulsory military service is one of the primary sources of not just Israel's military cyber but its civil prowess as well, and as such is a primary engine of economic growth.
- 12.2 Expand cyber education programs in schools and universities and improve adult education programs.
  - 12.21 Teach coding at least from elementary school through high school; Japan, Singapore, New Zealand, and Ireland already do so from kindergarten.[18]
  - 12.22 Add undergraduate degrees in cyber studies to the current graduate-level programs available at the different universities.
  - 12.23 Revise and expand training programs for under-represented populations (women, ultra-orthodox, Israeli Arabs), and provide incentives to hire graduates. Programs for these groups have met with limited success and require further consideration.
    - 12.23a Leverage cooperation with multinational tech firms. In 2022 Google announced a five-year investment of $25 million to promote increased opportunities for these under-represented groups and residents of Israel's periphery.[19]
- 12.3 Provide further inducements to staunch the brain drain of PhDs in critical areas. Many wish to stay or return but face a lack of appropriate

opportunity, especially in the universities. Comparatively small budgets can have an outsized impact.

- 12.4 Allow limited numbers of highly qualified foreign workers to be employed in Israel.
- 12.5 Provide a new pre-discharge cyber course for IDF soldiers to provide them with the skills needed for civilian employment. The new course would be similar to the one already offered to combat soldiers but would not be included as part of their compulsory service.
- 12.6 Promote Israel's character as a national cluster, already shown to be a critical factor in its cyber success (Chapter 8).
  - The INCD's Cybernet provides an important channel of communication; Cyber Week and other events bring people from the field together on an annual and ongoing basis; and various sub-clusters exist, such as the veteran's associations of IDF technological units.
    - 12.61 Expand existing means and develop new programs to further incentivize professional and social interaction within and between the governmental, military, business, and academic sectors.
    - 12.62 Provide minimal national coordination, to optimize the benefits, while preserving each subgroup's unique role.

Recommendation 13: Maintain Innovative Market-Based Regulatory System

Israel's informal national and business cultures are a critical component of its extraordinarily innovative high tech and cyber sectors. Israel has built a solid regulatory system that has helped promote an environment in which innovation can flourish. The rapidly evolving nature of the cyber realm means, however, that new and updated regulations, even legislation, will be needed on an ongoing basis.

- 13.1 Formulate clear objectives for the regulatory system, to chart a clear path forward and enable assessment of its performance.
- 13.2 Preserve appropriate balance between the regulatory and innovative needs of the cyber sector and high tech generally.
  - 13.21 Maintain the overall market-based approach, which seeks to impose minimal regulatory intervention. Care must be taken not to overly regulate business and stifle creativity.
  - 13.22 Enact uniform cyber regulations for all public and private sector entities, thereby reducing the regulatory burden, both in terms of administrative work and direct costs.

- 13.3 Develop incentives for regulatory compliance, such as tax breaks, reduced corporate liability, and preferential insurance rates.
  - Israeli law already contains precedents for incentives such as this, including subsidized automotive safety systems,[20] tax breaks to encourage investment in individual pension plans, or corporate tax write-offs for capital investment.
- 13.4 See additional recommendations regarding the regulatory system in Recommendations 19 and 26.

Recommendation 14: Get Serious about Turning Beersheba into a Major Cyber Hub

Population dispersal, including strengthening of the periphery, is critical for Israel for a variety of socioeconomic and national security reasons. Development, especially of the Negev, is an important part of Israel's national lore and societal resilience. The data suggest that the effort to turn Beersheba into a major cyber hub is stagnating. Resistance on the part of IDF intelligence and technological units, and their families, to the planned transfer to the Beersheba area is a major obstacle. Budgetary warfare over a small extension of a rail line has held up development of the entire region for years.

- 14.1 Invest massively in the transportation infrastructure to Beersheba and in the city as a whole to turn it into an attractive place for young couples to live, with an emphasis on IDF families.
- 14.2 Alternatively, stop throwing good money after bad. Other uses can be found for it.

Pillar 4—The 4Ds: Detect, Deter, Defend, Defeat

Recommendation 15: Maintain Cyber Intelligence Superiority

Rapid and accurate detection and attribution are particularly important in Israel's uniquely harsh threat environment, in which minor incidents can rapidly escalate into significant hostilities. The IDF Strategy stresses the importance of high-quality intelligence in the cyber realm, both for purposes of early warning (detection) and because of the cyber realm's important contribution to Israel's overall intelligence superiority. Effective detection is also crucial to deterrence, defense, and defeat of cyber threats. The number of sophisticated cyber adversaries Israel faces is relatively small, and it usually has intimate knowledge of their motivations and capabilities, thereby easing the attribution problem.

Private cyber security firms, both around the world and in Israel, have repeatedly played a critical role in identifying malware and their possible sources.

- 15.1 Ensure cyber intelligence superiority for purposes of detection and deterrence and to defend against threats before they can cause damage, as well as for offensive purposes.
- 15.2 Develop an agreed hierarchy of threats, as the basis for the intelligence collection plan (*tsiach*), and detailed operational plans for addressing those threats.
    - Doing so would provide for more effective allocation of resources for both cyber and kinetic operations and facilitate the work of interagency coordinating mechanisms. See also Recommendations 3.1 and 7.1.
- 15.3 Assure accurate attribution capabilities, in a politically and operationally relevant time frame.

  15.31 In periods of relative calm, Israel may be able to adopt somewhat more demanding levels of attribution, but even then these will have to be permissive by international standards. During periods of tension, they will, of necessity, have to be even more permissive.
- 15.4 Harness the capabilities of private cyber security firms (foreign and domestic) to augment governmental capabilities to detect and prevent attacks by foreign actors.
- 15.5 Strengthen mechanisms for exchanging information with public and private sector entities, to facilitate rapid detection of threats against them.

Recommendation 16: Formulate and Partially Declare a Mixed Kinetic-Cyber Deterrent Posture

Deterrence theory is elaborated on in Chapter 3. Deterrence by *denial* may be achieved by demonstrating, or credibly signaling, a state's ability to prevent an adversary from taking a certain action, thereby undermining its confidence in the utility of trying to do so. Deterrence by *retaliation* is based on the threat to punish the other side by causing significant harm, primarily to counter-value targets.[§§] All deterrence postures are difficult to achieve in the cyber realm, whether *explicit*, *indirect*, *quiet signaling*, or *symmetric*.

Escalation dominance requires the ability to deter an adversary without causing further intensification of a conflict. Kinetic attacks against counter-value

[§§] Counter-value targets refer primarily to population centers and other critical civilian sites, such as infrastructure; counter-force targets refer to military capabilities.

targets create a strong incentive to escalate and are thus typically deemed less suitable for purposes of escalation dominance than counter-force targets. In the cyber realm, however, counter-value targets may be attacked with minimal direct loss of life and so may be less escalatory.[21]

A declaratory posture is a statement of policy in a given area of military strategy. A cyber declaratory posture might include such issues as the types of conflicts in which cyber weapons would be used; the objectives behind offensive uses; intended responses to cyber attacks, whether by cyber or kinetic means or both; possible constraints on the uses of cyber weapons in times of peace and war; and how cyber capabilities are to be integrated into the state's broader military and national security strategies.[22] A declaratory posture can be achieved through a variety of formal statements, leaks, back-channel communications, and demonstrations of capability.

In practice, most states do not fully enunciate declaratory postures and a certain degree of ambiguity can be constructive. Both the United States and Russia, for example, have intentionally kept the threshold and nature of their intended responses ambiguous. NATO explicitly adopted a policy of cyber ambiguity, to deter opponents from crossing some unspecified line, but has intentionally refrained from stating what it might be and the nature of its intended response.

- 16.1 Formulate and enunciate at least the broad outlines of an *indirect* posture of mixed kinetic-cyber deterrence by *retaliation*, as set out in Recommendations 16–18, to ensure that adversaries have some understanding of the consequences they are likely to suffer, while maintaining ambiguity regarding Israel's overall capabilities and intentions.
- 16.2 Pursue cumulative process of mixed kinetic-cyber deterrence by *denial*, in which repeated failures create a sense of futility and ultimately weaken adversaries' resolve to continue trying.
    - 16.21 Ensure strong defensive capabilities and systemic resilience to diminish adversaries' prospects of success. Deterrence by denial in the cyber realm is intimately linked to defense and resilience.
- 16.3 Emphasize mixed kinetic-cyber deterrence by *retaliation* at higher-end cyber threats and by *denial* at low-intermediate threat levels.[23]
    - Deterrence by retaliation in all asymmetric conflicts, cyber and otherwise, is especially difficult at lower and intermediate threat levels.
    - The potentially less escalatory nature of cyber attacks against counter-value targets may provide Israel with an important new capability.
- 16.4 Develop a mixed range of kinetic and cyber responses, at the different rungs of the escalatory ladder.

  - The current ad hoc decision-making process does not maximize the range of options available to Israel. Not every response situation can be anticipated, but criteria for decisions can be formulated.
  - Standalone cyber deterrence and escalation dominance will rarely prove feasible. Israel's cyber deterrence will thus be a function of its overall deterrent posture, and the two will be mutually reinforcing.
- 16.5 Partially enunciate a pre-delegated retaliatory posture in response to devastating cyber attacks that may not be reliably attributable in an operationally and politically relevant timeframe.
  - Declaratory postures such as these are similar to those that states have been forced to adopt toward extreme threats in the physical world, such as nuclear terrorism.[24]

Recommendation 17: Integrate Cyber into Israel's Overall Deterrent Posture, Including Its Nuclear Strategy

The United States, and possibly the UK, have weighed a nuclear response to a cyber attack of devastating consequences. Concern has been expressed that the attack might also disable command-and-control systems before the defender was able to launch its nuclear forces. Furthermore, the defender might be deterred from launching a nuclear response, if the attack was perpetrated by a nuclear power.[25]

For reasons elaborated in Chapter 10, the kinetic feasibility of the Begin Doctrine—according to which Israel will take all measures necessary, including military, to prevent a hostile state in the region from going nuclear—is increasingly in doubt. Unlike with the Iraqi and Syrian nuclear programs, which Israel attacked from the air, Israel has yet to implement the doctrine in regard to the Iranian nuclear program, at least in the sense of an airstrike. Some question whether Israel has a viable kinetic option against the Iranian program at all. Stuxnet may have been an early harbinger of this changing reality.

- 17.1 Integrate Israel's cyber capabilities into its overall strategic deterrence posture including its nuclear strategy.
  - Systemic counter-value cyber capabilities could prove to be an effective deterrent, particularly at levels of conflict just below the existential, and provide Israel with a critical additional rung on the escalatory ladder.
- 17.2 Pursue cyber capabilities with systemic effects, as an addition to the Begin Doctrine's kinetic options for postponing and preventing the development of enemy nuclear weapons programs: Iran today, possibly others in the future.

Recommendation 18: Do Not a Adopt Policy of "No First Use"; Assure Second Strike Cyber Capability

In general, attacking first in the cyber realm provides unique advantages that may be lost by waiting, whereas absorbing a first strike affords a defender with greater international legitimacy to retaliate. This raises the question of whether to adopt a policy of "no first use" of cyber weapons. Israel has reportedly already "gone first" on at least two occasions, against the Syrian and Iranian nuclear programs.

A "second strike" cyber capability refers to a state's ability to respond devastatingly, even after absorbing a major strike against its cyber capabilities, whether by cyber or kinetic means. In the nuclear realm, from which the term is derived, a second strike capability is usually achieved by dispersing the actor's capabilities on a triad of land, sea, and air-based weapons systems. In so doing, a nuclear state seeks to deny an enemy the ability to eliminate its entire arsenal with a first strike and to deter it from even trying, given the likelihood that it will fail and suffer intolerable retaliation.

- 18.1 Do not adopt a policy of "no first use" of cyber weapons as part of possible international cyber norms and confidence building measures (CBMs).
  - The cyber realm is an area of unique Israeli advantage, at least for the foreseeable future.
  - In regard to international cyber norms and CBMs, see also Recommendations 24.31, 30.1, 30.2, 31.1, and 31.2.
- 18.2 Assure second strike cyber capability, including hardening, dispersal, and resilience of Israel's military cyber capabilities.

Recommendation 19: Strengthen Public and Private Sectors as First Line of Defense

Israel has built a comparatively effective civil cyber security system, and few attacks of national significance have taken place. Nevertheless, there continue to be important gaps in civil cyber security, as evidenced, inter alia, by the successful attacks against Israeli firms during 2020–2021 and inadequate oversight and supervision of critical national infrastructure.[26] Most of the attacks to date have not been sophisticated, and avoidable victim vulnerability, rather than attacker ingenuity, has usually been the source of failure. Cultural factors in Israel, such as a high tolerance for risk and tendency to disregard day-to-day administrative discipline, further exacerbate the problem.

The public and private sectors own and operate most of the infrastructure and networks in Israel's cyber realm and are thus the first line of defense. Only the government can defend against the most dangerous attacks, but most attacks can be stopped through straightforward improvements in cyber security that public and private sector entities can make on their own.

The INCD views itself more as a policy setting and professional guidance body than a regulatory enforcement agency. This approach stems, in part, from the belief that public and private sector entities will be less inclined to cooperate with it, of their own volition, if they are concerned that enforcement capabilities and penalties may ensue. The voluntary compliance approach has merit and may have been appropriate to the INCD's early years, but it is less so now that it has become an established government agency. Australia, for example has already passed binding legislation regarding information sharing with its cyber regulatory authority and both the United States and EU are considering doing so.[27]

- 19.1 Establish a rigorous national cyber risk management cycle and translate it into strategy, priorities, and budgets.[28]
    - 19.11 Adopt regulations *requiring* medium-large public and private sector organizations to:
        - 19.11a Develop cyber risk assessment, robustness, and resiliency plans[29] as part of the business licensing and renewal process or of planning and construction laws.
        - 19.11b Observe best practices in passive defense, such as cyber hygiene, malware blocking technology, automated patch management, strong encryption, and dispersal of information and key components.[30]
        - 19.11c Conduct cyber security training programs for all relevant employees.
    - 19.12 Require:
        - 19.12a Medium-large public and private sector organizations to share information with the INCD regarding cyber attacks conducted against them.
        - 19.12b Government IT systems to meet a realistic timeline for adopting the latest commercial capabilities for building defensible and resilient system architecture,[31] purchase hardware and software solely from verified sources, and make frequent changes to systems and networks as part of routine maintenance. (See Recommendation 26 regarding robustness and resilience.)
        - 19.12c Government contractors and vendors to meet cyber security standards and regulations established by the INCD and sectoral regulatory agencies.[32]

19.12d ISPs to act, both on their own and in conjunction with the INCD, to prevent and mitigate cyber attacks conducted through their services, including notifying users of attacks and taking corrective measures.

- 19.2 Strengthen INCD oversight and supervision over critical national infrastructure systems and other systems of major importance.
  - 19.21 Ensure actual enforcement of regulations and directives issued.[33]
  - 19.22 See additional regulatory recommendations in Recommendations 13 and 26.
- 19.3 Strengthen active and passive state-level defenses; conduct preventative cyber operations to disrupt and thwart attacks before and as they occur.
  - The United States and UK cyber strategies already call for proactive defense,[34] and Israel's unique security challenges leave it with few choices.
- 19.4 Ensure the cyber security of Israel's undersea communications cables and space-based Internet capabilities, which are particularly important vulnerabilities.[35]
  - Only three undersea communications cables connect Israel to the outside world, compared, for example, to the UK's 88,[36] which provide for far greater redundancy and resilience. Israel's space-based Internet capabilities (communications satellites and supporting infrastructure) are similarly limited.

Recommendation 20: Protect Electoral System and Freedom of Speech

Israel has not been the victim, to date, of successful cyber attacks designed to disrupt or influence its electoral processes, although attempts to do so have reportedly taken place. The existing electoral system, based on paper ballots, is outdated and cumbersome but essentially immune to cyber attack. This is not the case, however, of the parties' IT systems and websites and of some of the electoral machinery. The Central Elections Committee bears overall responsibility for the cyber security of the electoral process.

- 20.1 Assiduously preserve an open, free, multi-stakeholder approach to Internet and cyber realm governance generally, including freedom of discourse and respect of privacy rights.
- 20.2 Provide the senior functions of the executive, legislative, and judicial branches of government, the Central Elections Committee, and electoral machinery with defensive packages on a par with critical national infrastructure.
- 20.3 Appoint a special public council to advise the Central Elections Committee on electoral process cyber security.[37]

20.31 Make INCD professional guidance binding,[38] in practice at least should this not prove feasible in statute; a special SOC within CERT-Il might be dedicated to this.

- 20.4 Continue cooperating with multinational tech firms to block attempts to subvert Israel's democratic and electoral systems and conduct other malign information campaigns, for example, by removing sites and posts.

Recommendation 21: Counter Malign Cyber Influence Campaigns

As noted, we defined Israel's fundamental national consensus as one of the vital national security objectives and listed lesser, but still supremely important ones, at the beginning of this chapter. Considerable political controversy surrounds these objectives, though mostly about the means of achieving them not their basic substance. Israel's adversaries are clearly aware of the potential for significant disruption caused by influence campaigns and are likely to try to instigate some in the future.

- 21.1 Formulate a national strategy to counter malicious cyber influence campaigns that threaten Israel's fundamental national consensus, especially the integrity of its democratic and electoral systems.
  - The United States, UK, and France, among other democracies, have begun addressing this issue, Israel can learn from their experience.
- 21.2 Establish an inter-agency task force to formulate the strategy and coordinate proactive and reactive measures between all relevant civil and defense bodies.

  21.21 Place the task force under the supervision of a special public council, headed by a current or former supreme court justice, to avoid politicization.

  - Countering malign information campaigns is inherently sensitive in a democracy. The INCD, ISA, NSS, and other defense bodies cannot lead this sensitive and largely civil function.

Recommendation 22: License Select Entities to Conduct Regulated Hack Backs—Maybe

A state's right to take countermeasures in response to a wrongful act is explicitly recognized in international law and presumed to apply to the cyber realm as well. Generally speaking, countermeasures are only to be implemented after the injured state has asked the other to cease or remedy the wrongful act, but

international law does provide for immediate responses when necessary to avoid further damage. The situation becomes far more complex, however, when private entities are the targets of the attacks, especially critical entities, such as power companies, hospitals, dams, communications providers, and financial systems, whose disruption can have immediate, disastrous, and even fatal consequences.

In cases such as these, immediate and even autonomous computerized responses may be necessary to stop an attack and minimize the dangers of future ones. A requirement that the private entity await a governmental response to the attack, which may or may not be forthcoming and in any event may take time, or that it first consult with the relevant authorities and gain their approval before conducting a hack back, is obviously impractical. This thus raises the question of whether, and under what circumstances, private entities should be authorized to conduct hack backs on their own recognizance.

We are divided on this issue, as are other scholars, policy makers, and practicioners. One of us objects to any hack back authority whatsoever for non-governmental entities. While we all share the fear of cyber vigilantism, two of us believe that the recommended measures reduce the risks to an acceptable level.

- 22.1 License select private sector entities to conduct hack backs in carefully regulated circumstances and for highly circumscribed preventative purposes, as follows.
    - 22.11 Select private sector entities might include critical national infrastructure firms, ISPs, banks, cyber security firms, among others.
    - 22.12 Regulated circumstances might include cyber attacks that threaten a loss of life or a significant cut in critical services.
    - 22.13 Approval would be granted only to stop an attack in progress and prevent further damage and future attacks, and possibly to retrieve stolen data.
    - 22.14 Detailed regulations would have to be formulated to set out the criteria and restrictions on hack backs, as well as strict reporting and oversight measures.
    - 22.15 Hack backs by non-licensed entities or for purposes of retaliation or retribution would be strictly banned.

Recommendation 23: Adopt a Policy of Flexible Cyber and Kinetic Response

Both the United States and UK have adopted integrated, full spectrum, and flexible approaches, meaning that they reserve the right to take offensive action and respond by whichever means they deem appropriate, cyber or kinetic.[39] The fact

that Israel took credit for bombing Hamas's cyber operations center in 2019 is an indication that it, too, has adopted a flexible approach.

- 23.1 Adopt a policy of flexible cyber and kinetic responses and employ them as necessary, separately or in tandem, for offensive and defensive purposes.
- 23.2 Determine the nature of the response by the context and significance of the attack (critical or non-critical targets, level of damage actually caused, and escalatory potential), not whether it was cyber or kinetic. The following breakdown is not designed to be binding, but to serve as a general guideline for leaders' thinking.[***]
  - 23.21 Computer Network Attacks (CNA)—most such attacks (which disrupt, damage, and even destroy systems) can be deflected by defensive measures. When this is not the case:
    - Non-critical civilian and military systems—the response threshold should be relatively high and the response itself subject to considerations similar to those that govern kinetic attacks.
    - Critical civil and military systems—the response threshold for significant attacks against the former should be comparatively low, but the response potentially severe, for deterrence. For military systems, the threshold should be high and the strength of the response similar to kinetic attacks.
  - 23.22 Computer Network Exploitation Attacks (CNE)—the threshold and nature of the response should be similar as for other forms of espionage.
  - 23.23 Computer Network Influence Attacks (CNI)—the response threshold should be similar that for other information campaigns and the actual response should be primarily defensive.
    - Although the consequences of an information campaign would have to be severe to warrant a kinetic response of significance, the full spectrum of responses should be on the table, at least for purposes of deterrence.

Recommendation 24: Pursue Cyber Superiority and Ability to Inflict Systemic Disruption, Including through Cyber Information Operations

Standalone defeat of an adversary, in the traditional sense of preventing it from continuing to wage a conflict or undermining its psychological will to

[***] For greater detail on the nature of the different types of cyber attack, CNA, CNE, and CNI, see Chapter 1.

do so, is not usually achievable in the cyber realm. We thus proposed the concept of cyber superiority (see Chapter 3), that is, the ability to reduce the severity of attacks to a level that the state can tolerate and at which it can continue to function without significant disruption or to impose on an adversary a level of disruption or damage that it cannot tolerate. Cyber superiority and cyber deterrence are mutually reinforcing and exist along a continuum; there is not a black-and-white division between full deterrence or superiority and none at all. Whereas standalone cyber superiority will not usually prove feasible, it may be possible to achieve cumulative mixed-domain superiority.

Cumulative deterrence strategies do not work quickly, commonly entail painful setbacks, and require a degree of commitment that democracies can find difficult to sustain. Over a period of decades, Israel successfully established cumulative deterrence and military superiority over Arab states and may be in the process of doing so against Hezbollah and, less clearly, Hamas. Its ability to do so in the face of cyber threats remains to be demonstrated.

All of Israel's adversaries are authoritarian and, at least in the short term, may thus be less susceptible to information campaigns and attempts to interfere in their political systems. Some, however, particularly those with regimes under duress, may be vulnerable to counter-information campaigns designed to sow discord and even destabilize them.

- 24.1 Conduct intermittent engagement to achieve cyber superiority, rather than the higher US bar of continuous engagement to achieve cyber defeat.
  - Engagement with adversaries risks exposing Israel's cyber capabilities and increases the risks of escalation, particularly given the ongoing kinetic conflict with them.
- 24.2 Wield all elements of national power to achieve cyber superiority and, as appropriate, overall military defeat. Cyber superiority will be gained through a cumulative multidimensional combination of detection, deterrence, defense, and resilience, together with diplomacy and information operations.
  - Perception is critical; Israel's adversaries must believe that it will detect and prevent most attacks, that its defenses will ensure that those that do get through will not cause significant damage, or that resilience will lead to a rapid bounce back, and that retribution will be exacted.
- 24.3 Develop offensive cyber capabilities to inflict systemic disruption on critical enemy counter-value targets or to weaken and even destabilize regimes, including through information operations.
  - Systemic disruption requires the ability to damage critical infrastructure and other vital computer systems, promote domestic socioeconomic

turmoil, sow chaos and discord,[†††] exacerbate sectarian differences, or degrade a regime's ability to communicate with its public.

- Iran's oil industry, which constitutes a sizable portion of its overall GDP, including the oil infrastructure and shipping system, is an example of a particular vulnerability.

24.31 Reserve capabilities such as these primarily for war and other high levels of escalation. Food, water, and medical systems should *not* be targeted.

- Unlike nuclear capabilities, which can only be used—if at all—against imminent existential threats, cyber weapons may provide usable means of achieving systemic effects.
- The objective is to achieve practical tools of compellence and escalation dominance, for example, to force an adversary to terminate hostilities or change some other critical behavior.

24.32 Develop comparable capabilities against nonstate actors.

Recommendation 25: Develop Offensive Cyber Capabilities to Achieve Key Military Objectives with Precision and Minimal Collateral Damage

Hezbollah and Hamas intentionally deploy their military capabilities, especially rockets, in densely populated areas, using residents as human shields, thereby leading to civilian casualties when Israel seeks to destroy them. Israel goes to unusual lengths to minimize collateral damage in kinetic operations, but is nonetheless excoriated in the international media and public opinion. Israel has reportedly conducted numerous kinetic and cyber attacks against Iran's nuclear and missile programs, entrenchment efforts in Syria, and efforts to transfer advanced weapons to Hezbollah and other allies.

- 25.1 Develop tailored offensive cyber capabilities to disrupt and thwart key enemy military capabilities with precision and minimal collateral damage.[40]

25.11 Develop measures to disrupt critical counter-force targets, especially Iran's nuclear, missile, and drone programs and Hezbollah's precise rockets.

25.12 Develop measures to disrupt enemy command-and-control systems, that is, the civil and military leadership's ability to order forces into action and direct operations or to distort the forces' situational awareness.

- This may prove feasible primarily for larger conventional forces. Smaller formations and especially units of nonstate actors, for

[†††] For example, attacks designed to cast doubts on the integrity of financial systems or regimes' ability to ensure the provision of basic goods and services.

example, Hezbollah, are designed to operate autonomously precisely for this reason.

- 25.2 Develop the capability to target enemies' critical military infrastructure separately from the critical civil infrastructure, thereby creating new opportunities for counter-force denial.
  - An enemy's critical military infrastructure (electricity, water, communications) may be partly or, in some cases even completely, separate from the parallel civil infrastructure. This provides an opportunity to attack vital capabilities without causing civilian damage.
- 25.3 Cooperate with key international partners. See Recommendation 29.3.

Pillar 5—Aggregate Robustness and Systemic Resilience

Recommendation 26: Ensure Implementation of National Cyber Robustness and Resilience Plan

Aggregate robustness is designed to strengthen the public and private sectors' overall ability to repel and contain cyber attacks and continue functioning when under attack. Systemic resilience is designed to strengthen the state's ability to prevent and mitigate damage prior to, during, and following cyber attacks and to facilitate a rapid return to the antecedent level of functioning. Systemic resilience is necessary when robustness fails.[41] For more on robustness and resilience see Chapter 7.

Israel has long benefited from a sophisticated legal system, but actual enforcement has often been a weak point. The series of successful attacks against Israeli firms beginning in 2020 and, possibly even more worryingly, findings indicating that oversight even of critical national infrastructure has been deficient[42] raise questions regarding enforcement in the cyber realm as well. As noted, the INCD's voluntary compliance approach may have been appropriate to the its early formative years but is less so now that it has become an established government agency.

- 26.1 Ensure full implementation of the existing INCD robustness and resilience strategy.
  - 26.11 Assess and strengthen INCD organizational capabilities for promoting robustness and resilience.
  - 26.12 Turn the INCD into a regulatory enforcement agency, or propose an alternative enforcement mechanism, but end current equivocation.
  - 26.13 Enforce regulations requiring the public and private sectors to bear responsibility for managing their own cyber risk, including appointment of an official and board member responsible for cyber security.

- 26.2 Set clear resilience and robustness objectives for all governmental and public and private sector systems.[43]
  - 26.21 Within three years of program onset—all critical systems (Category A)[‡‡‡] to be resilient to known vulnerabilities and attack methods and fully implement INCD resilience and robustness directives.
  - 26.22 Within five years—all essential systems (Category B systems, i.e., those that are not on the critical national infrastructure list but still of great importance) to be resilient to known vulnerabilities and attack methods and fully implement INCD resilience and robustness directives.
  - 26.23 Within eight years—all government and public sector entities to fully implement INCD resilience and robustness directives and be resilient to known vulnerabilities and attack methods.
  - 26.24 Within eight years—national digital environment to be hardened to remove burden from the general public to the extent possible.
- 26.3 Implement strengthened risk management and regulatory system in Recommendation 19.1. Successful resilience is also a function of effective detection and defensive capabilities.
- 26.4 Seek rapid adoption of the new Cyber Law, to implement proposed hybrid regulatory system.

Pillar 6—International Cyber Cooperation, Influence, and Diplomacy

Recommendation 27: Leverage Cyber Cooperation to Promote Israel's Overall Foreign Relations

Israel's cyber prowess has become an important part of its national power and efforts to promote expanded diplomatic, economic, and military ties with states around the world. Nothing better exemplifies this than the Abraham Accords, in which cyber exports contributed to a dramatic change in Israel's strategic posture, including the establishment of formal and rapidly growing ties with the UAE, Bahrain, and Morocco and to growing informal relations with other Arab countries.

The government's clear recognition of the importance of international cyber cooperation and of active participation in international cyber discourse, notwithstanding, it has not fully availed itself of the opportunities in this area and

[‡‡‡] See three-tiered hybrid regulatory system proposed in new cyber bill, in Chapter 7.

its efforts do not enjoy sufficient funding, personnel, or central direction. The absence of any mention of the means by which international cyber cooperation is to be promoted in either the 2017 INCD National Cyber Strategy or the cabinet decisions is one of the existing strategy's primary weaknesses.

- 27.1 Continue leveraging cyber cooperation to promote Israel's foreign relations and national security objectives.
- 27.2 Formulate an international cyber outreach and cooperation plan.
  - 27.21 Prioritize states of particular importance, either because of their cyber capabilities, such as the UK, or for other reasons, for example, Germany, France, India, South Korea, and Japan. Cyber cooperation with the United States is addressed in Recommendation 28.
  - 27.22 Maintain careful balance between the strategic importance of Israel's emerging ties with Arab states and the potential harm to its values and overall foreign relations when cyber capabilities are abused by authoritarian regimes.
  - 27.23 Assist states of otherwise secondary importance to Israel, primarily in Africa and Latin America, where cyber cooperation may be leveraged to influence voting patterns in international organizations.
  - 27.24 Deepen strategic dialogue and expand practical cooperation with NATO in the areas of cyber R&D, education, training, and exercises and between its Cyberspace Operations Center and CERT-IL. NATO's Industry-Cyber Partnership may be a basis for expanded commercial ties with Israeli firms.[44]
- 27.3 Expand international cyber training programs in Israel, possibly in cooperation with private sector firms.
  - 27.31 Establish an international cyber education program for foreign students and practitioners, maximizing the expertise of the different universities in Israel.
  - 27.32 Provide scholarships and fellowships for foreign students and practitioners to study and work in Israel.
    - Programs such as these are the modern-day equivalent of Israel's highly successful agricultural outreach efforts during its early decades.
    - 27.4 Provide appropriate funding for international cooperation programs. Even modest budgets may have an outsized impact on Israel's international standing.

Recommendation 28: Deepen and Institutionalize Civil and Military Cyber Cooperation with the United States

The United States is Israel's primary partner in the cyber realm and the two countries engage in extensive cooperation at all levels, civil and military. Unlike most other areas of military cooperation with the United States, Israel's cyber capabilities are primarily indigenous, and it has much to offer, not just gain. Israel thus seeks to further expand bilateral cyber cooperation, but also to maintain its freedom of independent action, part of the emphasis that its strategic culture has long placed on the principles of strategic autonomy and self-reliance. A significant expansion of the already broad bilateral cyber cooperation will require coordination at the level of the White House and Prime Minister's Office.

Ad-hoc cooperation between the United States and Israel, in a variety of areas, has proven very effective over the years, and formal agreements are harder to reach. Nevertheless, formal agreements have the advantage of providing more binding policy guidance for officials, easing allocation of funds by the US Congress, and establishing the basis for long-term cooperation. Israel already conducts extensive commercial and counterterrorism ties with a number of US states, not just the federal government. Some big cities, especially New York, even have major cyber programs of their own.

- 28.1 Develop multi-year plan setting out Israel's objectives for civil and military cyber cooperation with the United States, both in the near term and over the next three to five years.
- 28.2 Institutionalize a formal and permanent structure of cyber dialogue and cooperation.
    - 28.21 Establish a Senior Cyber Working Group, as the lead forum for bilateral cyber dialogue.[§§§]
        - 28.21a Establish working groups in all relevant civil agencies, for an exchange of expertise, policy approaches, best practices, and practical cooperation.
        - 28.21b Establish a Senior Defense Cyber Working Group to integrate cooperative efforts between all relevant US and Israeli military and intelligence cyber agencies. Both this and the working groups, would report to the Senior Cyber Working Group.
    - 28.22 Integrate the cyber dialogue into the overall strategic dialogue, chaired by the respective national security advisers and heads of state.

[§§§] At the time of this writing, under the Biden Administration, the appropriate US official would be the deputy national security advisor for cyber and emerging technologies. The Israeli counterpart would be the head of the INCD.

- 28.3 Formalize both civil and military cyber cooperation in new and expanded MoUs.
  - 28.31 Seek further upgrades of the 2016 cyber MoU between the Department of Defense and Ministry of Defense and/or of the various cooperation agreements between the operational agencies directly involved.
  - 28.32 Maximize the potential of the 2014 US-Israel Strategic Partnership Act, which provides for heightened cooperation in various areas, including cyber security, and which directed the president to report to Congress on potential areas of cyber security cooperation.[45]
  - 28.33 Complete legislation adding cyber to the US commitment to maintain Israel's qualitative military edge (QME).
- 28.4 Pursue the deepest possible bilateral operational and intelligence cyber cooperation without exposing Israel's unique capabilities or constraining its freedom of independent cyber action.
- 28.5 Actively participate in US-led efforts to form a coalition of democratic countries to collectively defend against cyber threats.[46]
- 28.6 Seek greater access to US federal cyber contracts, civil and military, and cooperation at state and local levels.
  - 28.61 Establish a joint mechanism to approve Israeli participation in federal cyber contracts, if necessary, on a case by case basis. Report cases of rejection to the Senior Cyber Working Group for resolution.
    - For security reasons, including lingering US mistrust stemming from past Israeli espionage (the 1987 Pollard Affair), Israeli firms are largely shut out of federal cyber security contracts. In contrast, Israeli participation in weapons development and manufacturing contracts is extensive.
  - 28.62 Promote cyber cooperation at state and local levels, not just the federal.
- 28.7 Do *not* seek a US cyber security guarantee or standalone cyber treaty.
  - Consideration has been given to the desirability of a possible US military cyber guarantee, whether akin to the 1998 bilateral missile defense MoU or otherwise, and even of a standalone cyber treaty.
  - Israel's independent cyber capabilities are sufficient, and it does not wish to be constrained by limitations on its freedom of action. Cyber cooperation and a cyber guarantee might, however, be components of an overall defense treaty, should one be considered in the future.

Recommendation 29: Conduct Focused Diplomacy and Military Cooperation to Counter Cyber Threats

Israel's diplomatic efforts and international military cooperation have long focused on the nuclear, rocket, and terrorist threats posed by Iran, Hezbollah, and Hamas. The cyber threat has yet to receive attention commensurate with its growing magnitude. Israel's rapidly expanding ties with Arab countries, following the historic Abraham Accords, have paved the way for heretofore unimaginable areas of cooperation.

- 29.1 Accord cyber higher priority in Israel's diplomatic efforts to counter the threats posed by Iran, Hezbollah, and Hamas.
    - 29.11 Leverage cyber cooperation with states around the world, as set forth in Pillar 6, to promote diplomatic campaigns against Iranian, Hezbollah, and Hamas cyber capabilities.
    - 29.12 Include cyber in the anti-Iran axis evolving between Israel and Sunni states.
- 29.2 Assist select states in promoting the defense and resilience of their civil and military cyber realms.
    - 29.21 Help develop national cyber strategies and institutions; provide intelligence, technology, and expertise regarding passive and active defense measures, cyber exercises, and more.
    - 29.22 Establish a regional CERT to assist national ones when their capabilities prove insufficient.
        - Israel's growing ties with Arab states make the plausibility of a regional CERT far greater.
        - Broader Mediterranean and/or European CERTs might also be established, as might be CERTs by industry, for example, automotive, airlines, and pharmaceuticals.[47]
- 29.3 Conduct joint offensive operations with a very select group of states against common adversaries. Seek the ability to "defend forward," including detection and pursuit of adversaries on partner networks.[48]
- 29.4 Launch an initiative with Arab partners to promote digital economies throughout the Middle East.
    - 29.41 Leverage the Abraham Accords to promote a vision of a peaceful and prosperous Middle East based on advanced digital economies.
    - 29.42 Promote a regional development program together with regional and international partners and funders.

Recommendation 30: Adopt Positive but Cautious Approach to International Cyber Norms, CBMs, and Law

Israel's level of cyber dependency is far greater than that of its adversaries, and an effective rules-based international order might work at least partially in its favor, as it has in the comparatively professional and nonpoliticized deliberations of the International Atomic Energy Agency. For the most part, however, international cyber norms and agreements are likely to prove even less effective than existing arms control regimes have. Iran, Iraq, Libya, and Syria are signatories to the NPT, but pursued nuclear weapons programs, nevertheless, and probably also had chemical weapons programs despite the Chemical Weapons Convention. Further exacerbating the verification challenge, cyber weapons are far easier to hide, a plethora of nonstate actors have cyber capabilities, not just states, and states may not have full control over all hackers acting at their behest or from their territory.[49]

- 30.1 Adopt a fundamentally positive but cautious approach toward international cyber norms, agreements, and laws.
- 30.2 Support international cyber norms, agreements, and laws designed, inter alia, to:
    - 30.21 Promote national cyber capacity building.
    - 30.22 Safeguard an open and free multi-stakeholder approach to Internet and cyber governance.
    - 30.23 Ban cyber attacks, in peace and wartime, against targets whose direct and immediate consequence is a loss of civilian life, such as air traffic control systems, autonomous vehicles, or medi-tech and hospitals; in peace time, ban cyber attacks against critical national infrastructure and against electoral systems.

Recommendation 31: Play Active Role in Multilateral Cyber Forums

International norms, law, and agreements are only now evolving in the cyber realm. Israel has an opportunity to demonstrate good international citizenship in an area where it is a global leader, establish its role as such, and help shape developments in positive directions, or at least reduce the potential for harm. Israel will not be recognized as a global leader in the cyber realm while taking a backseat in global cyber discourse.

- 31.1 Play an active role in multilateral cyber forums.

31.11 Actively support the Western open, free, multi-stakeholder approach to Internet and cyber realm governance and encourage a values-driven debate about technology and society generally.

31.12 Help shape emerging discourse on the applicability of the Law of Armed Conflict to the cyber realm, for example, that the right to self-defense applies to cyber attacks by nonstate actors, not just states, and that states have the right to respond to cyber attacks with cyber and/or kinetic means.

31.13 Minimize the potential negative impact of emerging norms, treaties, and law on Israel's unique advantages in the military cyber realm and freedom of action, for example, with a ban on the first use of cyber weapons[50] or on cyber attacks against specific categories of targets, with the exception of those noted in recommendation 30.23

- 31.2 Support US, UK, and other efforts to promote universal adherence to voluntary norms of responsible state behavior during peace time, including practical CBMs.[51] CBMs of importance to Israel might include:
  - An international and/or regional cyber hotline,[52] to reduce the dangers of misperception and escalation and to help diffuse potential crises.
  - Addition of cyber to future regional security forums.
  - Informal understandings with Israel's adversaries regarding the "rules of the game," or unilateral limitations on cyber attacks, for example, the suggested ban on cyber attacks resulting in direct and immediate loss of civilian life.
  - International and/or expert working groups and forums designed to promote greater understanding in the cyber realm.
- 31.3 Play an active role to revitalize and expand the Digital 5 Group of Leading Digital Governments, an informal grouping of states with prominent records in digital government.
  - Israel was a founding member of the group, which now counts 10 members but appears to have stagnated in recent years.
- 31.4 Further expand existing cyber cooperation with multinational organizations, such as the OECD, World Bank, African Union, and UN.

Recommendation 32: Conduct Cyber Dialogue with Major Multinational Tech Firms

Israel's relations with some of the multinational tech giants (including Microsoft, Facebook, and Google) have been adversely affected by employee protests regarding the Palestinian issue and over the NSO scandal. In many areas, these firms' cyber capabilities and resources exceed those of state actors, including

Israel's, and they play an increasingly important role in establishing international cyber norms and regulations. Israel's civil and military capabilities stand to suffer significant adverse consequences, and it cannot afford to find itself in a state of tension with them.

- 32.1 Conduct intensive dialogue with the major multinational tech firms and take measures to assuage their concerns.

Recommendation 33: Seek to Expand Ties with China but Accord Priority to the United States; Establish Compulsory Foreign Investment Oversight Mechanism

China has become Israel's second largest trading partner after the United States (though as a bloc, the EU is the largest) and is a leading investor in Israel's cyber industry and high tech sector generally. The United States has expressed deep misgivings over Chinese investments in Israel in transportation and other civil infrastructure, and especially in the cyber area, including 5G and a variety of other advanced technologies. US pressure in the late 1990s and early 2000s led to a cessation of all Israeli military cooperation and sales to China. In more recent years, the United States has demanded that Israel also curtail its relations with China in these commercial areas and strengthen oversight of them. Israeli-Chinese ties have slowed as a result.

- 33.1 Accord clear priority to ties with the United States, Israel's irreplaceable strategic partner, but seek to preserve and further expand ties with China, which is of increasingly critical importance for Israel economically and strategically.
  - This recommendation requires difficult balancing between conflicting US and Chinese interests. Israel's efforts to do so have fully placated neither side to date and are unlikely to do so in the future.
  - The priority given to the United States and consequent blow to ties with China is the painful price of an extraordinary relationship with the former.
- 33.2 Complete establishment of a *mandatory* oversight mechanism for foreign investment in Israel's high tech and cyber sectors to address US concerns.
  - 33.21 Deepen involvement of NSS in oversight of foreign investment in Israel in general and in the high tech and cyber areas in particular.
    - Unlike the Finance Ministry, which has borne primary responsibility for this to date and in which financial considerations predominate, the NSS is directly subordinate to the premier and attaches primacy to national security considerations.[53]

- The initial impetus for this recommendation was US concern regarding Israel's ties with China, however, its rapidly growing ties with formally hostile states, such as the UAE and Bahrain, make an effective foreign investment oversight mechanism that much more important generally.

33.22 Seek at least partial compensation for losses in commercial ties with China through enhanced trade with the United States and greater access to US federal contracts.

- See detailed proposals in this regard by Greenert and Bird.[54]

Recommendation 34: Strengthen Organizational Capabilities to Promote International Cyber Cooperation

- 34.1 Strengthen the role of the Ministry of Foreign Affairs (MFA) in cyber diplomacy.

  34.11 Upgrade the level of the MFA cyber official to ambassadorial status, so as to be on a par with foreign counterparts, and expand the portfolio to emerging technologies and scientific affairs generally.

  34.12 Provide appropriate training to MFA diplomats to maximize their ability to promote Israel's cyber interests. Include cyber in all professional MFA training courses, from diplomatic cadets up.

  34.13 Develop a cyber diplomats corps—officials from various parts of the civil and military bureaucracy and volunteers from the public and private sector to be sent to represent Israel in all relevant international cyber forums—legal, academic, commercial, policy, and standards.

  - To be a global cyber power, Israel must be active in all cyber forms of significance.
  - Personnel constraints mean that the MFA cannot represent Israel appropriately in all cyber forums of importance. For the price of travel costs and minimal training in international affairs and diplomacy, the cyber diplomats corps can represent Israel in the various forums.
- 34.2 Establish an international cyber development assistance agency, whether as part of the MFA's Department of International Assistance (MASHAV) or the INCD to provide centralized direction for all Israeli efforts in this area.
  - A truly effective, mission-focused effort to promote international cyber cooperation would probably be best established within the INCD.
- 34.3 Strengthen the INCD's international cooperation organizational capabilities in order to carry out the out expanded role envisaged for it herein, with or without Recommendation 34.2.

- 34.4 Promote dissemination of both international cyber cooperation programs and Israel's cyber strategy.
  - In the absence of such documents, in English and preferably additional languages, some states are unaware of the benefits they may derive from cooperation with Israel and of its contribution to international cyber discourse and to the cyber realm as a whole.

Appendix

COMMON TYPES OF CYBER ATTACKS

Denial of Service (DoS) Attacks—aim to make a machine or network resource inaccessible to anyone attempting to access it and are among the most common type of attack. The perpetrator seeks to "flood" the network with more access requests than it can process at one time, resulting in either a decrease in network speed or an inability to access the site at all.

Distributed Denial of Service (DDoS) Attacks—unlike DoS attacks, which are perpetrated by a single individual or computer, a DDoS attack uses hundreds or thousands of computers to attack a single computer or network. To make matters more complicated, the perpetrator may carry out the attack by hijacking other computers remotely without the knowledge of the person who owns the machine. DDoS attacks are inexpensive but can have significant effects for their victims. If the DDoS attack cannot be disrupted or diverted, the victim might even be forced to replace and upgrade hardware in order to address the attack. In 2016 a US-based anti-ISIS hacktivist group claimed responsibility for what may have been the biggest DDoS attack ever committed up to that time, shutting down all BBC websites for several hours.[1] Arguably the most famous DDoS attack was on Estonia in 2007, which had severe effects on Estonia's government, banks, and other networks and their ability to provide services to citizens.

Malware—is an umbrella term for any computer software that is designed to cause damage to a machine or network. Malware aims to disrupt normal computer functions and can also allow an external user to hijack the machine and take control. Malware can corrupt or destroy data and in some cases can self-replicate in order to spread further or to grow larger so there is no space left on the hard drive.

A **worm** is a type of malware that lies dormant until accessed, when it utilizes information transfer systems to spread from one computer to another. The spread of the worm may allow for multiple computers to be remotely controlled.

Stuxnet, Duqu, and Flame are all examples of worms, as discussed in detail earlier in the book. Worms remain a commonly used form of malware.[2]

A **logic bomb**, unlike other forms of malware, can remain dormant for a long period of time. The "bomb" is set off when certain conditions are met, such as the passing of a set amount of time, or the failure of the victim to respond to a certain command. In 2013 a logic bomb, possibly employed by either a hacker group or North Korea, crashed the servers of three TV networks and two major banks in South Korea, causing them to shut down temporarily.[3]

A **Trojan horse** is any malware that disguises itself as legitimate software, thus tricking the user into downloading or installing the program. One example is a Trojan horse that disguises itself as an anti-virus program, while actually introducing viruses onto the victim's computer. Once it has gained access, the Trojan horse can create backdoors, spy, steal passwords and credit card information, delete, block, copy or modify data, disrupt computer performance, or even take over and lock the victim out of their computer entirely. In contrast to other forms of malware noted above, Trojan horses cannot self-replicate.[4]

Ransomware is a form of malware in which the attacker blocks access to a network or machine until a ransom, or sum of money, is paid. In many cases, the ransom is demanded in Bitcoin (XBT), an electronic currency that is difficult to trace.[5] These attacks are growing in frequency. In the first 10 months of 2019, for example, at least 140 local governments (including the city of Atlanta), hospitals, and police stations fell victim to such attacks.[6] These types of attacks can end up mimicking DoS attacks as they also block access to machines and networks until the ransom is paid.

Polymorphic malware encompasses any type of malware that modifies its identifiable features each time it replicates in order to avoid detection. Polymorphic malware is capable of repeatedly modifying itself without further commands. It can include viruses, worms, bots, trojan horses, or keyloggers.[7] The overwhelming majority of malware has at least some polymorphic ability.[8]

A **botnet** refers to a network of private computers remotely controlled by malware without their owners' knowledge. Botnets are a key component of DDoS attacks.

Drive-By Downloads—refer to when a user unintentionally downloads malware of any type onto their computer, for example, from an infected webpage. Drive-by downloads can infect machines by utilizing exploits in a browser, app, or operating system that have not yet been patched.[9]

Watering Hole—this is a strategy employed by malicious actors that utilizes drive-by downloads to infect computers and networks of particular organizations or individuals. A watering hole strategy involves attempting to figure out which websites people from a targeted organization are likely to use and looking for vulnerabilities in those sites. Once a vulnerable website is found the

attacker injects corrupted JavaScript or HTML that redirects users to a website the attacker has infected with malware. The goal is for someone from the organization to access the corrupted site and thus be made to inadvertently download the malware, which grants the attackers access to that targeted network or machine.[10]

Phishing—these are some of the most common attacks, when malicious actors send emails to individuals that are made to look like they originate from a company or government agency in an attempt to trick the recipient into providing passwords or other private information. The goal can be espionage or to gain access to a network in order to install malware.

Spear Phishing—shares the same methodology and goals as phishing but instead of targeting a broad audience, emails are sent to specific individuals, companies, or organizations. One subset of spear phishing, known as **whaling** attacks, target only high-ranking officials in companies or government agencies.

Injections—this refers to an attempt to introduce (or inject) new code into a computer program. The goal of the effort is to modify the functioning of the computer program. Code injection is conducted by gaining access to a system and exploiting an unpatched security vulnerability in a software program.[11] These attacks have a wide range of purposes from disabling or damaging security programs to easing the spread of malware to stealing, blocking access to, altering, or deleting data.

SQL (Structured Query Language) Injections—are a common form of injection attack. SQL refers to a computer language that is used for database management. SQL injections thus specifically target databases and attempt to allow the attacker to gain access. If successful, the attacker, depending on what the database system is designed to do, can then modify the database, void transactions, change balances, pretend to be the legitimate user, delete or make data unavailable, or copy or disclose the information in the database.[12]

Eavesdropping

Eavesdropping's objective is to intercept electronic or digital communications of an individual or organization without their knowledge. It often takes the form of **network eavesdropping**, which involves using programs that record packets of communications data from targeted networks. The attacker then will decode that data, including breaking cryptographic protections if needed, to learn what information the data holds. Some forms of communication are particularly vulnerable, including Voice over IP and wireless networks, as well as any organization that uses a central hub to organize all communications.[13]

Spoofing

Spoofing is when an attacker attempts to use a disguised form of communication to deceive a recipient into believing the communication originates with a trusted or known source. This can be done through email, phone calls, websites, and more sophisticated techniques including manipulated IP addresses, Address Resolutions Protocols, or Domain Name System servers. Spoofing has a number of uses. It can grant access to personal information and passwords, be used to spread malware, or bypass network access controls, as part of a DoS attack or as part of a broader attack such as an advanced persistent threat (more on this below).[14]

Backdoor

A backdoor refers to a way in which actors can gain access to a network or computer by going around existing security measures. Attackers can either uncover flaws in existing coding that allows for unauthorized access or can upload malware that creates a backdoor. Once inside the attackers can use a backdoor to steal information, surveil a network, infect the network with malware, or even take control of the device. Once attackers have discovered a backdoor, they will generally attempt to keep their presence a secret so that it is not noticed.[15]

Cross-Site Scripting (XSS)

XSS is a form of script injection attack in which malicious scripts, often called malicious payloads, are injected into a legitimate website or web application. Through the vulnerabilities of the website or web application, the malicious payload can then be delivered to the browser of website visitors and web application users. XSS is one of the most prevalent website security threats, with the most widely used medium being JavaScript, in addition to VBScript, ActiveX, and Flash.[16] There are three major types of XSS attacks.

Password Hack

There are many ways for an attacker to discover his victim's password and use it to access private information. Some include:

The **brute force attack**, in which the hacker uses a script or program to try commonly used passwords, such as "password," "Password123," and so on until one works.

The **dictionary attack**, in which the hacker uses a script or program to cycle through combinations of words from the dictionary. The program only tries those combinations most likely to succeed, a method which exploits the fact that most people choose short (less than 7 character) passwords consisting of one or two words.

The **keylogger attack** is malware that records every keystroke a user makes and exports that data to the attacker. It is used to steal any information the user types, including things like passwords, on the targeted machine. It is more dangerous than the brute force or dictionary attack, because stronger passwords do not defend against it.[17]

Multi-factor authentication (MFA, or alternatively 2FA—two-factor authentication) is a cyber defense mechanism that requires a user to provide not just a password but also a secondary security factor. Such a set up makes hacking into a computer or network far more difficult.

Advanced Persistent Threat (APT)

APT attacks consist in gaining unauthorized access to a system or network and remaining there for an extended period of time without the victim's knowledge. As implied by its name, the APT often incorporates multiple advanced types of attack, including those discussed here, implemented in several phases so as to avoid detection and maximize the duration of the attack. APTs are extremely dangerous because they "fly under the radar" of traditional cybersecurity measures and allow for huge amounts of data to be stolen over a long period of time.

APT attacks can have the same goals as other types of attacks. Some aim to steal data, others to disrupt normal functioning and operation; they can even aim to destroy infrastructure. The main difference is that in the case of an APT the objective is to do so over a period of months or even years rather than right away. This heightens the dangers these attacks pose as the effects are on-going rather than time limited.

The malware for APT attacks is designed and customized with a specific target in mind. APT attacks represent a huge threat to both corporation and governments, because they are highly sophisticated and specifically tailored to outmaneuver the security mechanisms of the targeted system (as opposed to common viruses directed against many different targets).[18]

Zero-Day Exploit

A zero-day (or zero hour or day zero) exploit is a cyber attack that takes advantage of a security flaw in a computer system or network for which there is no patch. Zero-day exploits attack vulnerabilities the developers of the software or hardware are not aware of, and thus have not yet been able to fix. As a result, such attacks are extremely difficult to detect. Once the flaw or attack is discovered, developers can then quickly patch it, but until then, zero-day exploits can be used by attackers to cause severe damage to a computer or network.[19]

LIST OF INTERVIEWS

Tom Ahi Dror, former senior official, INCD
Major General (ret.) Nitzan Alon, former head of IDF Operations Branch
Amit Ashkenazi, legal advisor, INCD
Sagy Bar, head of Cyber Education Center
Arik Barbing, former senior official, ISA cyber division
Prof. Major General (ret.) Isaac Ben-Israel, former head of Cyber Task Force, head of MoD R&D Division
Brigadier General (ret.) Dani Bren, former senior IDF officer, C4I Branch
Brigadier General (ret.) Pinchas Buchris, former director-general, Ministry of Defense
Buky Carmeli, former head of INCD
Lt. General (ret.) Gadi Eisenkot, former IDF chief of staff
Major General (ret.) Amir Eshel, director-general, Ministry of Defense, former commander of IAF
Major General (ret.) Yair Golan, former IDF deputy chief of staff
Tal Goldstein, former senior official, INCD
Yoram Hacohen, CEO Israel Internet Association
Ronen Korman, former head of ISA Operational Technology and Cyber Branch
Noam Krakover, former senior official, INCD
Prof. Eviatar Matania, former head of INCD
Dan Meridor, former minister of finance, justice and intelligence affairs
Ilan Mizrachi, former deputy head of Mosssad
Iddo Moed, cyber affairs, Ministry of Foreign Affairs
Major General (ret.) Uzi Moscowitz, former head of IDF C4I Branch
Dr. Deganit Paikowski, Hebrew University
Tamir Pardo, former head of Mossad
Brigadier General (ret.) Yaron Rosen, former head of IDF Cyber Defense Brigade

Brigadier General (ret.) Ehud Schneorson, former head of Unit 8200
Dr. Roy Schondorf, Deputy Attorney General (International Law)
Dr. Amit Sheniak, Hebrew University
Dr. Lior Tabansky, Tel Aviv University
Lior Yaffe, head of INCD operations branch
Roi Yarom, senior official, INCD
Prof. Tal Zarsky, Haifa University
Amitai Ziv, *The Marker*

NOTES

Prologue

1. *Times of Israel* 2015; https://www.gov.il/he/departments/news/press_19022019; http://bit.ly/2Ni9OWD; https://www.idfblog.com/2017/01/02/model-city-trains-coders-stop-hacks/; https://www.ynetnews.com/articles/0,7340,L-4683636,00.html.

Introduction

1. Adapted from: United States of America, 2018.1.
2. Ben Zion Gad, *Jerusalem Post*, January 12, 2022; *The Marker*, Haaretz, June 26, 2016; Ezra Kreiner and Joe Charlaff, *Jerusalem Post*, December 28, 2017; Alon Ben-David, *Aviation Week and Space Technology*, June 27, 2011.57; Clarke and Knake 2010.155; Graumann 2013.66; Eisenstadt and Pollock 2012.35; David Shamah, *Times of Israel*, July 9, 2014; Shuker and Siboni 2019.27–28; David Horovitz, *Times of Israel*, February 6, 2019.
3. Jonathan Silber, *YNET*, January 26, 2012; Hirshoga and Toker 2012; Khazan 2012; Zippori 2012.
4. Jonathan Silber, *YNET*, January 26, 2012; Hirshoga and Toker 2012; Khazan 2012; Zippori 2012; "Cyberattacks on Israel Rose Exponentially in the Past Four Years," *Haaretz*, June 16, 2016; Joe Charlaff, *Jerusalem Post*, December 28, 2017; Alon Ben-David 2011.57; Simone Shemer, *NoCamels*, January 29, 2020; *Jerusalem Post* Staff, June 7, 2020; TOI Staff, *Times of India*, May 19 and June 1, 2020.
5. James Vincent, *The Independent*, July 29, 2014; Hirshoga and Nati Toker, *The Marker*, November 22, 2012; Olga Khazan, *Washington Post*, November 17, 2014; Siboni et al. 2013.7; Michal Zippori, *CNN*, January 26, 2012; Nati Toker, *Tech Nation*, January 22, 2012; Stuart Winer, *Times of Israel*, August 17, 2014; Jack Moore, *Newsweek*, April 7, 2015; Stuart Winer, *Times of Israel*, Aril 7, 2015.
6. Fiona Willian, *9 News*, July 2, 2019; "Eurovision Song Contest—Statistics and Facts," *Statista*, September 16, 2019; Nor Dvori, *HaMadura HaMerkazi*, January 26, 2019; TOI Staff, *Times of Israel*, January 26, 2020; *Jerusalem Post* Staff, March 20, 2022.
7. *Times of Israel*, January 30, 2018.
8. TOI Staff, "Iran Duped Pakistan into Israeli Nuclear Threat as Tiny Part of Huge Fakery Campaign," September 6 and November 30, 2018.
9. Yoav Zitun, *YNet*, July 24, 2019.
10. Gili Cohen, *Haaretz*, March 23, 2016.
11. Yaniv Kobovich, *Haaretz*, July 4, 2008; Tal Shahaf, *Ynet*, May 8, 2019.
12. Even and Siman-Tov 2012.36.
13. Amos Harel, *Haaretz*, July 9, 2017; Amos Harel, *Haaretz*, July 13, 2017; Yaniv Yakubobich, *Haaretz*, January 13, 2019.

14. Yonah Jeremy Bob, *Jerusalem Post*, February 25, 2019.
15. Cora Currier and Henrik Moltke, *The Intercept*, January 28, 2016.
16. Even and Siman-Tov 2012.37; Jonathan Silber, *YNetnews.com*, January 26, 2012; Cohen and Levin 2014a; Siboni and Kronenfeld 2014; Valeriano and Maness 2015.170–171; Armin Rosen, *Business Insider*, August 18, 2014; Mohammed J. Herzallah, *Newsweek*, July 27, 2009; David Shamah, *Times of Israel*, July 9, 2014.
17. Mohammed Herzallah, *Newsweek*, July 27, 2009.
18. Mohammed Herzallah, *Newsweek*, July 27, 2009.
19. Siboni et al. 2013.7; Or Hirshoga and Nati Toker, *The Marker*, November 22, 2012; Michal Zippori, *CNN*, January 26, 2012.
20. Nati Toker, *Tech Nation*, January 22, 2012; Or Hirshoga and Nati Toker, *The Marker*, November 22, 2012; Olga Khazan, *Washington Post*, November 17, 2012.
21. Yaakov Lappin, *Jerusalem Post*, November 19, 2010; Richard Silverstein, *Tikan Olam*, May 11, 2013.
22. Yoav Limor, *Israel Hayom*, February 7, 2019.
23. Bernard Brode, *The Times of Israel*, December 18, 2020.
24. Bebber 2016.
25. www.worldometers.info/computers/; https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/; Government of the United States, Department of Homeland Security 2018.2.
26. Government of the United States, Department of Homeland Security 2018.2; Shoshana Solomon, *Times of Israel*, January 31, 2018.
27. Bebber 2016.
28. Mike Isaac and Sheera Frenkel, *New York Times*, September 28, 2018; Brian Fund, *Washington Post*, September 26, 2018; "Cyberattack on Equifax Leaves 143 Million Consumers Compromised," *Nickels/McHugh/McHugh*, September 8, 2017; Nicole Perlroth, *New York Times*, October 3, 2017; Tiffabu Hsu, *New York Times*, September 7, 2017; *The Economist*, September 16, 2017. 14.
29. Grant Gross, *Internet Society*, February 23, 2018; Shoshana Solomon, *Times of Israel*, January 31, 2018; Argaman and Siboni 2014; Maynard and Beecroft 2015; Mohurle and Patil 2017.
30. David Sanger, Nicole Perlroth, and Julian Barnes, *New York Times*, May 9, 2021; Gerrit De Vynck and Rachel Lerman, *Washington Post*, July 3, 2021; Ellen Nakashima and Rachel Lerman, *Washington Post*, May 15, 2021; Nicole Perlroth, *Washington Post*, June 5, 2021.
31. David Sanger, *New York Times*, July 27, 2018; David Sanger and Emily Schmall, *New York Times*, February 28, 2021; Siboni and Kronenfeld 2013.31; Siboni et al. 2020.22; Dena Temple Raton, *NPR*, September 26, 2019; Nicole Perlroth, *New York Times*, October 23, 2020; Courtney Kube, Carol E. Lee, Dan De Luce, and Ken Dilanian, *NBC News*, July 20, 2018.
32. Michael Schmitt, *Just Security*, December 21, 2020.
33. David Sanger and Sharon LaFraniere, *New York Times*, December 3, 2020; James Purtill, *Australian Broadcasting Company*, December 14, 2020; Guy Davies, *ABC News*, July 20, 2020; Government of the United Kingdom, National Cyber Security Center. "Advisory: APT29 Targets Covid-19 Vaccine Development," 2020; Agnus Liu, *Fierce Pharma*, December 10, 2020; Alex Scroxton, *ComputerWeekly.com*, December 10, 2020.
34. Conti and Raymond 2017.1.
35. Clarke and Knake 2010.30.
36. Clarke and Knake 2010.17–21; Segal 2017.67–77; Rid 2013.7–9; Cohen 2013.10–17; Andrew Kramer, *New York Times*, January 14, 2022.
37. Jasper 2017.42; Clarke and Knake 2010.53; Sanger 2018.67–68.
38. Harris 2014.xiv; Segal 2017.7, 63, 140.
39. Jasper 2017.37, 40; Sanger 2018.127, 130–131, 136–137, 286–287, 289; David Sanger and Nicole Perloth, *New York Times*, April 20, 2020; K. J. Kwon, *CNN*, April 22, 2015; *The Economist*, May 20, 2017.67–68; Nadan Feldman, *The Marker*, August 4, 2017.18–19.
40. Lin and Zegart 2019.121–122; Dena Temple Raton, *NPR*, September 26, 2019; Sanger 2018.132, 271–274, 278; David Sanger and William Broad, *New York Times*, November 16,

2017; David Sanger and Eric Schmitt, *New York Times*, June 12, 2017; Idrees Ali and Phil Stewart, *Technology News*, October 16, 2019; Jasper 2017.66.

41. Sanger 2018.50; Loudermilk 2019; Reuters, *New York Times*, December 9, 2012.
42. David Sanger and Nicole Perlroth, *New York Times*, May 28, 2021; Jasper 2017.22; Healey in Lin and Zegart 2019.182–183; Zolan Kanno-Younfs and David Sanger, *New York Times*, July 20, 2021.
43. David Sanger, Edward Wong, and Jason Horowitz, *New York Times*, July 28, 2020; Chico Harlan and Stefano Pitrelli, *Washington Post*, July 29, 2020.
44. Cory Dickstein, *Stars & Stripes*, October 4, 2019; Anderson and Sadjadpour 2018.31, 40.
45. Segal 2017.7–9; Government of the United States 2020.9–10, 17; Rosenberger 2020.
46. Rosenberger 2020.
47. Ronen Bergman and Farnaz Fassihi, *New York Times*, September 18, 2020.
48. Sanger 2018.18; Tim Starks, *Politico*, September 10, 2020.
49. Sanger 2018.24, 184–186, 211, 218–223, 226, 231–232, 239; Jasper 2017.21; Daisuke Wakabayashi and Scott Shane, *New York Times*, September 27, 2017; Craig Timberg and Tony Romm, *Washington Post*, December 16, 2018; Julian Barnes, *New York Times*, December 21, 2018; Tim Starks, *Politico*, September 10, 2020.
50. Julian Barnes and David Sanger, *New York Times*, October 21, 2020; Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, *Washington Post*, October 21, 2020; Ellen Nakashima, Amy Gardner, and Aaron Davis, *Washington Post*, December 22, 2020; Tabatabai 2020.11; Miles Parks, *NPR*, June 4, 2020; Tabatabai 2020.15–16.
51. Segal 2017.39, 46.
52. Baram 2013.24; Tabansky 2020; Graumann 2012; Eisenstadt and Pollock 2012.xiii, 2; Steinherz 2014; Energy Secretary Ernest Moniz, "Conference of the National Committee for Energy in Tel Aviv," April 2016; Benoliel 2015. 443.
53. Graumann 2012.
54. International Institute for Strategic Studies 2021.
55. Baram 2017.1–10.
56. Farwell and Rohozinski 2011; Even and Siman-Tov 2012; United States Army Command and General Staff College 2014, Parmenter 2013. 39.
57. Carr 2012; Clarke and Knake 2012.
58. Taylor 2016.143–144, 220, 229–230; Adamsky 2010.113–114, 126; Baram and Ben-Israel 2018.
59. Freilich 2012.33–35.
60. This is a well-established phenomenon in Israel, referred to by numerous sources, but see Senor and Singer 2009.
61. Morgenthau 1948; Waltz 1954; Waltz 1979; Mearsheimer 2001; Walt 2002.
62. Buchanan 2017.2–4, 6, 64, 80, 96; see also NATO Parliamentary Assembly, Science and Technology Committee 2019.12.
63. Buchanan 2017.2–4.; Slayton 2016/2017.72–73.
64. Mueller 2010; Mueller et al. 2013.98; Clarke and Knake 2012.
65. Demchak and Dombrowski 2011.
66. Government of the United States, White House 2017.13; Government of the United Kingdom 2016.47; NATO Parliamentary Assembly, NATO Parliamentary Assembly, Science and Technology Committee 2019.4, 10.; Farrell and Glaser in Lin and Zegart 2019.48; Clarke and Knake 2012.195.
67. Siboni 2013.7.
68. Taylor 2016.217, 220, 229–230.
69. Freilich 2012 and 2018; Adamsky 2010.113, 115.
70. Wendt 1992 and 1999; Finnemore 1996; Keck and Sikkink 1998.
71. Eriksson and Giacomello 2006.236; Hansen and Nissenbaum 2009.
72. Eriksson and Giacomello 2006.233.
73. Isnarti 2016.160; Deibert and Rohozinski 2010; Lupovici 2016.339; Hansen and Nissenbaum 2009.
74. Adamsky 2010.6; Adamsky 2019.1–2.

75. Freilich 2018; Adamsky 2010.113, 115.
76. Harknett and Goldman 2016.83.
77. Sanger 2018.xx.

Chapter 1

1. Rid and McBurney 2012.8.
2. Israel Government Decision no. 3611 of August 7, 2011; https://www.pcmag.com/encyclopedia/term/62535/dod-cyberspace-glossary.
3. Kausch and Tabansky 2018.2.
4. Harris 2014.149, 155.
5. Kenney, 2015.113; https://apps.dtic.mil/dtic/tr/fulltext/u2/a439217.pdf p. II-2; Kevin Coleman, "Cyber Terrorism," *Directions Magazine*, 10 October 2003, https://www.directionsmag.com/article/3655; Buchanan 2017.
6. Buchanan 2017.35; Jasper 2017.5.
7. Jasper 2017.4, 32; NATO Parliamentary Assembly 2019.2; Conti and Raymond 2017.4.
8. Clarke and Knake 2010.182.
9. Buchanan 2017.35–36.
10. Rid 2013.36–37, 39–41.
11. Jasper 2017.6.
12. Kenney 2015.115; Rid and Buchanan 2015.6; Valeriano and Maness 2015.26, 33.
13. Segal 2017.17–18.
14. Clarke and Knake 2010.11–70.
15. NATO Parliamentary Assembly 2019.5; Demchak 2011; Valeriano and Maness 2015.26–27.
16. Tabansky and Ben-Israel 2015.2.
17. Linda Rosencrance, *TechTarget*.
18. Siboni and Assaf 2016.10.
19. Linda Rosencrance, *TechTarget*; Siboni and Assaf 2016.10; Siboni et al. 2013.10–16.
20. https://csrc.nist.gov/glossary/term/computer_network_attack; Lorents and Ottis 2010.135; Lin and Zegart 2019.69–70; Lindsay 2013.371.
21. https://csrc.nist.gov/glossary/term/computer_network_exploitation; Nye 2016/2017.47.
22. Singer and Friedman, 2014.91–92; Valeriano and Maness 2015.35, 68; Rid 2013.82; Lindsay 2013.370.
23. Clarke and Knake 2010.81, 124; Rid 2015.82.
24. Siboni and Assaf 2016.21; Dombe, *Israel Defense*, July 7, 2016; IAI Press Release, *IAI*, June 17, 2018; Government of the United Kingdom, Parliament 2021.
25. Valeriano and Maness 2015.3; Hathaway et al. 2011.
26. Singer and Friedman 2014.69.
27. Nye 2011.236; Clarke and Knake 2010; Carr 2012; Demchak 2011; Kello 2013.23, 26; Zetter 2014; James Bamford, *Wired.com*, June 12, 2013.
28. David Sanger, Nicole Perlroth, and Julian Barnes, *New York Times*, May 9, 2021; Gerrit De Vynck and Rachel Lerman, *Washington Post*, July 3, 2021; Ellen Nakashima and Rachel Lerman, *Washington Post*, May 15, 2021; Nicole Perlroth, *Washington Post*, June 5, 2021.
29. Interview, Tamir Pardo.
30. Jeremy Straub, *LiveScience.com*, August 27, 2019; Government of the United States 2014; Clarke and Knake 2010.
31. Francis Robles and Nicole Perlroth, *New York Times*, February 8, 2021.
32. Yonah Jeremy Bob, *Jerusalem Post Magazine*, December 10, 2020.
33. Redins, *RISK Management*, December 5, 2012; Nye 2011.212.
34. House of Representatives Joint Hearing 2013.2, 12, 39; Office of the President 2009.1–2; Clarke and Knake 2010.31, 70, 170; Carr 2012.20; Zetter 2014.
35. Mueller 2010; Mueller et al. 2013.
36. Chris Bing, *Cyber Scoop*, November 15, 2016.; Jeremy Hsu, *IEEE Spectrum*, March 26, 2014; Stan Schroeder, *Mashable*, February 14, 2018.
37. Herr 2014.7; Siboni 2015; Bussolati 2015; Siboni et al. 2013; Rid and McBurney 2012.12; Lindsay 2013.

38. Herr 2014.7; *The Economist*, May 20, 2017.68.
39. Ablon et al. 2014.ix; Lindsay, 2013.375, 376.
40. Harris 2014.103–105.
41. Ablon et al. 2014.x; Lindsay 2013.370.
42. Rattray and Healey 2011; Kello 2013.36; Jonathan Silber, *YNetNews.com*, January 26, 2012; Siboni et al. 2013.10–16.
43. Siboni et al. 2013.8, 17–18.
44. Bussolati 2015; Ablon et al. 2014.ix; Siboni et al. 2013.10, 11.
45. Kello 2013.25; Mueller 2010; Mueller et al. 2013.86–104; Nye 2011.207–208; Perkovich and Levite 2017.172.
46. Gartzke and Lindsay 2014.9.
47. Lin 2018.66; Lindsay 2013.378–379, 396–397; Barzashka 2013.51; Herr 2014.8.
48. Government of the United Kingdom 2016.19.
49. Kenney 2015.123.
50. Schweitzer et al. 2013.21; Clarke and Knake 2010.136.
51. BBC Staff, *BBC News*, January 23, 2018; Natasha Lomas, *TechCrunch,* January 24, 2018.
52. Daphne Benoit and Didier Lauras, *Barron's*, June 2, 2021.
53. Brian Bennett, *Time Magazine*, June 7, 2021.
54. Matania et al. 2016.78; Conti and Raymond 2017.54–55.
55. Jasper 2017.4; Conti and Raymond 2017.4; Brantly 2018.26–27.
56. Perkovich and Levite 2017.162–164, 250.
57. Segal 2017.19; Government of the United States 2020.28; Brad Smith, *Microsoft,* December 17, 2020.
58. Segal 2017.19; Government of the United States 2020.28; Brad Smith, *Microsoft,* December 17, 2020.
59. Amitai Ziv, *The Marker*, October 1, 2017; Harris 2014.220; Rid 2013.viii, 114; Segal 2017.19, 31; Mueller et al. 2013; Jasper 2017.73; Sanger 2018.xii–xiii; David Sanger, *New York Times*, June 16, 2018; Matania et al. 2016.78; Brad Smith, *Microsoft*, December 17, 2020.
60. Clarke and Knake 2010.31.
61. Buchanan 2017.42.
62. Kello, 2013.36; Jonathan Silber, *YNetNews.com*, January 26, 2012; 2015 DoD Cyber Strategy, cited in Cilluffo and Clark 2016.7; Bebber 2016.
63. Segal 2017.12.
64. Matania et al. 2016.78; Clarke and Knake 2010.31; Kello, 2013.22.
65. Constance Douris, *Forbes*, Feb 6, 2018.
66. Even and Siman-Tov 2012.19; Rid 2013.viii.
67. United States Army Command and General Staff College, 2014.4; David Sanger, *New York Times*, June 16, 2018; Perkovich and Levite 2017.45, 116; Fischerkeller and Harknett 2017.382.
68. Even and Siman-Tov 2012.32–33; Libicki 2009.xiv-xv; Clarke and Knake 2010.45, 51; Silber, *YNetNews.com*, January 26, 2012.
69. Libicki in Lin and Zegart 2019.137; Long in Lin and Zegart 2019.121.
70. Gartzke 2013.43; Gartzke and Lindsay 2017; Rid 2013.
71. Cherry 2005.72–73; Cohen and Levin 2014b; Gartzke 2013; Harknett 2018; Nye 2016/2017.45; Siboni et al. 2013; Valeriano et al. 2018.18–19; Weimann 2005.
72. Klein 2018; Libicki 2009; Milevski, 2011; Weinmann 2006.
73. Brantly 2018.106; DeVore and Lee 2017.41; Smeets 2017.9, 21–22; Goines 2017.98; Syadjari 2004.
74. Bates 2020.21; DeVore and Lee 2017.40; Kello 2013; Silber 2012; Smeets 2018.26; Valeriano et al. 2018.5.
75. Bates 2020.26–27; Corn and Jensen 2018.127–128; DeVore and Lee 2017.44; Hatch 2018.52, 54; Healey 2019b.11; Jensen and Valeriano 2019.3; Koh 2017; Lindsay 2013; Mueller et al. 2019.112; Perez 2009.6–7; Rid and Buchanan 2015; Rovner 2019; Valeriano et al. 2018.18, 76.
76. Bates 2020.22; Straub 2019.3; Demchak and Dombrowski 2011.
77. Bellovin et al. 2017.60.
78. Rovner 2019.

Chapter 2

1. Clarke and Knake 2010.30.
2. Segal 2017.67–73; Rid 2013.6–7; Clarke and Knake 2010.11–16; Ian Traynor, *The Guardian*, May 16, 2007; Tabanksy and Ben Israel 2015.
3. Segal 2017.67–77; Rid 2013.7–9; Clarke and Knake 2010.17–21; Cohen 2013.10–17.
4. Sanger 2018.154–155.
5. Ben Farmer, *The Telegraph*, February 15, 2018; Christopher Miller, *Radio Free Europe*, March 7, 2018; Sarah Marsh, *The Guardian*, February 15, 2018; Alfred Ng, *CNET*, February 15, 2018; Andy Greenberg, *Wired*, August 22, 2018; Buchanan 2017.78; Sanger 2018.4, 156; Andy Greenberg, *Wired.com*, September 14, 2019.
6. Andy Greenberg, *Wired*, June 6, 2017; Sanger 2018.157–160, 169.
7. Bebber 2016.
8. Andy Greenberg, *Wired*, June 6, 2017; Sanger 2018.157–160, 169.
9. Andrew Kramer, *New York Times*, January 14, 2022.
10. Sanger 2018.xvi, 5, 164; Nicole Perlroth and David Sanger, *New York Times*, March 15, 2018; Nicole Perloth, *New York Times*, July 6, 2017; Gross et al. in Lin and Zegart 2019.238; Jasper 2017.44; Frances Robles and Nicole Perlroth, *New York Times*, February 8, 2021; Nicole Perloth and Clifford Krause, *New York Times*, March 15, 2018; Elias Groll, *Foreign Policy*, December 21, 2017; David Sanger, *New York Times*, July 27 and October 23, 2018; David Rose, *The Mail*, September 17, 2018; Arial Davis, *MIT Technology Review*, March 5, 2019.
11. Michael Schmidt and Nicole Perlroth, *New York Times*, October 19, 2020.
12. David Kirkpatrick and Ron Nixon, *New York Times*, April 16, 2018.
13. Sanger 2018.20; Harris 2014.146, 149–150.
14. Evan Perez and Shimon Prokupecz, *CNN*, April 8, 2015; Sanger 2018.187, 189.
15. Sanger 2018.226–227.
16. Zachary Cohen, Luke McGee, and Alex Marquardt, *CNN*, July 16, 2020; Julian Barnes, *New York Times*, July 16, 2020.
17. David Sanger and Nicole Perlroth, *New York Times*, December 8, 2020.; David Sanger, *New York Times*, December 13, 2020; Ellen Nakashima and Joseph Marks, *Washington Post*, December 8, 2020.
18. The section on the SolarWinds attack is a composite picture of the following sources: David Sanger, *New York Times*, December 8 and December 13, 2020; David Sanger and Nicole Perlroth, *New York Times*, December 14 and December 17, 2020; David Sanger, Nicole Perlroth, and Eric Schmitt, *New York Times*, December 15, 2020; David Sanger, Nicole Perlroth, and Julian Barnes, *New York Times*, December 16, 2020, and January 2, 2021; Nicole Perlroth, *New York Times*, December 31, 2020; Ellen Nakashima, *Washington Post*, December 31, 2020; Ellen Nakashima and Joseph Marks, *Washington Post*, December 8, 2020; Ellen Nakashima and Craig Timberg, *Washington Post*, December 14, 2020; Christopher Bing, *Reuters*, December 13, 2020; Hannah Murphy, *Financial Times*, December 18, 2020; Dustin Volz and Robert McMillan, *Wall Street Journal*, December 17, 2020; Jaclyn Diaz, *NPR*, December 24, 2020; Jason Aten, *Business Insider*, December 21, 2020; Laura Hautala, *CNET*, December 24, 2020; Jody Westby, *Forbes*, December 16, 2020; Sam Ingalls, *ESecurity Planet*, December 18, 2020; Fred Kaplan, *Slate*, December 18, 2020; Michael Schmitt, *Just Security*, December 21, 2020; Herb Lin, *Lawfare*, December 22, 2020; Kim Zetter, *The Intercept*, December 24, 2020; Reuters, *DW.com*, December 18, 2020; Brad Smith, *Microsoft.com*, December 17, 2020.
19. David Sanger and Nicole Perlroth, *New York Times*, May 28, 2021.
20. David Sanger and Nicole Perlroth, *New York Times*, May 28, 2021; Audrey Conklin, *Fox Business*, May 28,2021; Robert McMillan and Dustin Volz, *Wall Street Journa*l, October 25, 2021.
21. Sanger 2018.211, 218–223, 239; Jasper 2017.21; Daisuke Wakabayashi and Scott Shane, *New York Times*, September 27, 2017; Craig Timberg and Tony Romm, *Washington Post*, December 16, 2018.
22. Sanger 2018.24, 184–186, 202, 212–213, 218–223,226, 231–232, 238–239; Adam Goldman, *New York Times*, October 19, 2018; Jonathan Chait, *National Interest*, August 3, 2019; Georgia

Wells et al., *Wall Street Journal*, October 8, 2019; Craig Limburg and Tony Romm, *Washington Post*, December 16, 2018, and July 25, 2019; Tim Starks, *Politico*, September 10, 2020.

23. Yoram Rosner and David Siman-Tov, *INSS*, Insight #1031, March 8, 2018; Shamir and Bachar, *Israel Democracy Institute*, January 2019.10; Melissa Eddy, *New York Times*, September 10, 2021.
24. Julian Barnes and Sidney Amber, *New York Times*, February 21, 2020; Nicole Perlroth and David Sanger, *New York Times*, September 27, 2020; David Sanger and Zolan Kanno-Youngs, *New York Times*, September 22, 2020; Julian Barnes, Nicole Perlroth, and David Sanger, *New York Times*, October 22, 2020; US National Intelligence Council, March 10, 2021.
25. Harris 2014.64.
26. Segal 2017.7–9; Sanger 2018.105, 244; Government of the United States 2020.9.
27. Sanger 2018.105–106; Clarke and Knake 2010.57; Segal 2017.33–34; Jasper 2017.43.
28. Raymond Zhong, Paul Mozur, Jeff Kao, and Aaaron Krolik, *New York Times*, December 19, 2020; L. Rosenberger, *Foreign Affairs*, 2020.
29. Dakota Cary, *Defense One*, July 23, 2021.
30. David Sanger, *New York Times*, March 20, 2021; Government of the United States 2020.9–10, 17; L. Rosenberger, *Foreign Affairs*, 2020.
31. Government of the United States 2020.9–10, 17; L. Rosenberger, *Foreign Affairs*, 2020.
32. L. Rosenberger, *Foreign Affairs*, 2020.
33. Segal 2017.7–9; Sanger 2018.105, 244; Government of the United States 2020.9.
34. David Sanger and Steve Erlanger, *New York Times*, December 18, 2018.
35. Harris 2014.xiv; Segal 2017.7, 63, 140.
36. Government of the United States 2020.9; Nicole Perlroth and David Sanger, *New York Times*, July 20, 2021.
37. David Sanger and Emily Schmall, *New York Times*, February 28, 2021.
38. Sanger 2018.101; Jasper 2017.42; Government of the United States 2020, p. 10.
39. Government of the United States 2020, p.9; Zolan Kanno-Younfs and David Sanger, *New York Times*, July 20, 2021.
40. Nicole Perlroth, David Sanger, and Scott Shane, *New York Times*, May 6, 2019.
41. Sanger 2018.109.
42. David Sanger and Steve Erlanger, *New York Times*, December 18, 2018.
43. David Sanger, Edward Wong, and Jason Horowitz, *New York Times*, July 28, 2020; Chico Harlan and Stefano Pitrelli, *Washington Post*, July 29, 2020.
44. Ellen Nakashima, *Washington Post*, March 6, 2021; David Sanger, Julian Barnes and Nicole Perlroth, *New York Times*, March 7 and March 14, 2021; Zolan Kanno-Younfs and David Sanger, *New York Times*, July 20, 2021.
45. Sanger 2018.18.
46. Harris 2014.154; Government of the United States, National Intelligence Council, 2021.7.
47. Abigail Grace, *Foreign Policy*, October 4, 2018; Government of the United States 2020.68.
48. Raymond Zhong, Paul Mozur, Jeff Kao, and Aaaron Krolik, *New York Times*, December 19, 2020; L. Rosenberger, *Foreign Affairs*, 2020.
49. Bebber 2016.
50. Sanger 2018.103.
51. Robert R. Kim, "North Korea Policy One Year after Hanoi," *Center for Strategic and International Studies*, May 15, 2019.
52. Jasper 2017.37, 40; Sanger 2018.127, 130–131, 136–137; Government of the United States 2020.13; International Institute for Strategic Studies 2021.
53. Sanger 2018.140–144, 150; Segal 2017.57–67; Haroon Siddique and Agencies, *The Guardian*, January 5, 2015; Staff and Agencies, *The Guardian*, December 23, 2014; David Brunnstrom and Jim Finkle, *Reuters*, December 18, 2014.
54. K.J. Kwon, *CNN*, April 22, 2015.
55. Sanger 2018.286.
56. Michelle Nichols, *Reuters*, August 5, 2019; David Sanger and Nicole Perlroth, *New York Times*, April 15, 2020.; Government of the United States 2020.13.
57. Scott Ikeda, *CPO Magazine*, September 3, 2020.

58. Sanger 2018.287, 289; *The Economist*, May 20, 2017.67–68; Nadan Feldman, *The Marker*, August 4, 2017.18–19.
59. K. J. Kwon, *CNN*, April 22, 2015.
60. Laura Dobberstein, *The Register*, June 21, 2021.
61. Sanger 2018.287.
62. Segal 2017.xix, 149.
63. Long in Lin and Zegart 2019.121–122
64. Dena Temple Raton, *NPR*, September 26, 2019; Nicole Perlroth, *New York Times*, October 23, 2020.
65. David Sanger, *New York Times*, February 24, 2014.
66. Sanger 2018.39.
67. Jasper 2017.66.
68. David Sanger and Julian Barnes, *New York Times*, September 23, 2019; Julian Barnes, *New York Times*, August 28, 2019.
69. Idrees Ali and Phil Stewart, *Technology News*, October 16, 2019.
70. David Sanger and Julian Barnes, *New York Times*, September 23, 2019.
71. Scott Shane, *New York Times*, November 2, 2013.
72. Barbara Starr, *CNN*, June 25, 2019.
73. Sanger 2018.241, 244–247; Rosenbach et al. 2021.
74. Sanger 2018.132, 271–274, 278; David Sanger and William Broad, *New York Times*, November 16, 2017; David Sanger and Eric Schmitt, *New York Times*, June 12, 2017.
75. David Sanger and Zoan Kanno Youngs, *New York Times*, September 22, 2020.
76. Ellen Nakashima, *Washington Post*, December 25, 2019, and October 9, 2020; David Sanger and Nicole Perlroth, *New York Times*, October 12, 2020; Mark Pomerleau, *C4ISRNET*, October 30, 2020.
77. Segal 2017.xix, 149.
78. Dana Priest, Craig Timberg, and Souad Mekhennet, *Washington Post*, July 18, 2021; Harris 2014.70–71, 93, 94, 96.
79. Sanger 2018.241, 244–247.

Chapter 3

1. Kello 2013.8; Siboni and Kronenfeld 2012.
2. Government of the United States, White House 2003.
3. Government of the United Kingdom 2016; Government of the United Kingdom 2022.
4. Freilich 2018; Cohen et al. 2016; Freilich 2015; Government of Israel, Office of the Chief of Staff 2015.
5. Government of the United States, White House 2018; Government of the United States, White House 2017; Government of the United States, Department of Defense, US Cyber Command 2018; Government of the United States, Department of Defense 2015; Clarke and Knake 2010; Buchanan 2017.
6. Liff 2012; Nye 2016/2017; Ben-Horin and Posin 1981.vii.
7. Donnelly et al. 2019.55.
8. Clarke and Knake 2010.157; Long in Lin and Zegart 2019.106–107.
9. Jasper 2017.15.
10. Long in Lin and Zegart 2019.106–107.
11. Farrell and Glaser in Lin and Zegart 2019.48; Sanger 2018.xix, 289, 297; Clarke and Knake 2010.189, 192, 195.
12. Jervis 2016.70.
13. Jasper 2017.112, 130; Libicki 2009; Sanger 2018.32.
14. Jervis 2016.68.
15. Jervis 2016.69.
16. Fischerkeller and Harknett 2018. 381, 386.
17. Jasper 2017.10.
18. Jasper 2017.11; Jervis 2016.70–72.

19. Sanger 2018.289; Clarke and Knake 2010.193–194; Jasper 2017.11; Jervis 2016.70–72.
20. Freilich 2018.
21. Perkovich and Levite 2017.170.
22. Clarke and Knake 2010.156.
23. Healey in Lin and Zegart 2019.182–183.
24. Government of the United States, White House 2017.13; Government of the United Kingdom 2016.47; NATO Parliamentary Assembly, Science and Technology Committee 2019.4, 10.
25. Government of the United States, White House 2017.17.
26. Government of the United States, Department of Defense 2015; Government of the United States, White House 2003; Government of the United States, White House 2017; Government of the United States, White House 2018; Government of the United Kingdom 2016.
27. NATO Parliamentary Assembly, Science and Technology Committee 2019.12.
28. Kugler 2009.
29. Jasper 2017.11.
30. Harris 2014.50; Sanger 2018.303–304; Clarke and Knake 2010.46; Healey in Lin and Zegart 2019.176.
31. Government of the United States, Department of Defense 2015.
32. Healey in Lin and Zegard 2019.176–178.
33. Jervis 2016.68; Slayton 2016/2017.108; Fanelli 2016. 63.
34. Libicki 2009; Donnelly et al. 2019.57–62.
35. Jervis 2016.66; Donnelly et al. 2019.57–62.
36. Pamment 2019; Freilich 2018.172.
37. Donnelly et al. 2019.57–58.
38. Perkovich and Levite 2017.211, 213, 216, 219.
39. Singer and Friedman 2014; Government of the United States, Department of Defense, Defense Science Board 2017; Government of the United Kingdom 2016.47.
40. Government of the United States, Department of Defense, Defense Science Board 2017.6.
41. Applegate 2012; Even and Siman-Tov 2012.32–33; Libicki 2009.xiv–xv, 136; Clarke and Knake 2010.45, 51; Jonathan Silber, *YNetNews.com*, January 26, 2012; Nye 2016/2017.48; Jasper 2017.10; Rid 2013; Liff 2012; Joint Advanced Warfighting School 2014.
42. Rid and Buchanan 2015; Gross et al. in Lin and Zegart 2019.239; for sources on the US response to the Sony attack and attempted sabotage of Iran's missile program, see Chapter 2.
43. Lindsay 2013.400.
44. Rid and Buchanan 2015.7.
45. Buchanan 2017.143; Rid 2013.160, 170.
46. Eilstrup-Sangiovanni 2018.
47. Jasper 2017.89.
48. Long in Lin and Zegart 2019.117, 121.
49. Buchanan 2017.143–147; Davis et al. 2017.20, 29.
50. Brantly 2018.181.
51. Moran 2012.
52. Government of the United States, White House 2003.
53. Ingis in Lin and Zegart 2019.27–28, 3; Healey 2019b.11.
54. Zrahia 2014.
55. Brantly 2018.106; Cohen et al. 2017.
56. Farrell and Glaser in Lin and Zegart 2019.57–58; Sanger 2018.141.
57. Australian Government 2009.
58. Healey 2019a.22.
59. Buchanan 2017.2–4.
60. Buchanan 2017.2–4, 6, 64, 80, 96; see also NATO Parliamentary Assembly, Science and Technology Committee, 2019.12.
61. Even and Siman-Tov 2012.20.
62. Buchanan 2017.5; Even and Siman-Tov 2012.20; Parmenter 2013. 4,10; Nuriel 2011.
63. Farrell and Glaser in Lin and Zegart 2019.47, 58–60, 63.

64. Sanger 2018.17.
65. Buchanan 2017.2–4, 6, 64, 80, 96; see also NATO Parliamentary Assembly, Science and Technology Committee 2019.12.
66. Jervis 2016.72; Government of the United States, Office of the Under Secretary of Defence for Acquisition: Technology and Logistics 2017.10; NATO Parliamentary Assembly, Science and Technology Committee 2019.11–12; Eilstrup-Sangiovanni 2018.
67. Slayton 2016/2017.72–109.
68. Eilstrup-Sangiovanni 2018.
69. Eilstrup-Sangiovanni 2018.
70. Deibert and Rohozinski 2010; Valeriano and Maness 2015.191; Zittrain 2008.70; Sofaer et al. 2010.180.
71. Borghard and Lonergan 2019.122–145; Kreps and Schneider 2019.
72. Government of the United States, Office of the Under Secretary of Defence for Acquisition: Technology and Logistics 2017.15.
73. Jensen and Valeriano 2019.2, 3, 12; Josh Rovner, *War on the Rocks*, September 16, 2019.
74. David Sanger and Nicole Perlroth, *New York Times*, May 28, 2021; Jasper 2017.22; Healey in Lin and Zegart 2019.182–183; Zolan Kanno-Younfs and David Sanger, *New York Times*, July 20, 2021.
75. David Sanger, *New York Times*, February 1, 2022.
76. Valeriano et al. 2018. 76; Jensen and Valeriano 2019.3; Josh Rovner, *War on the Rocks*, September 16, 2019.
77. Jensen and Valeriano 2019.2, 3, 12; Kreps and Schneider 2019; Fischerkeller and Harknett 2019.
78. Healey 2019b.2, 13–15; Fischerkeller and Harkness 2019.
79. Borghard and Lonergan 2019.122–145.
80. Borghard and Lonergan 2019.122–145; Catalin Cimpanu, *The Record,* May 19, 2021; BBC Staff, *BBC*, June 9, 2021; Tal Shachaf, *YNet*, May 21, 2021.
81. Idrees Ali and Phil Stewart, *Technology News*, October 16, 2019; David Sanger and Julian Barnes, *New York Times*, September 23, 2019.
82. Farrell and Glaser in Lin and Zegart 2019.48, 51; Kreps and Schneider 2019; Healey in Lin and Zegart 2019.187.
83. Farrell and Glaser in Lin and Zegart 2019.49–50.
84. Fanelli 2016.54–56, 59.
85. Government of the United States, Department of Defense 2018; Government of the United States, Department of Defense, US Cyber Command June 2018.5–6; Harknett 2018.
86. Healey 2019b.13–14; Harknett and Goldman 2016.96.
87. Harknett and Goldman 2016.85.
88. Jasper 2017.10; Lindsay 2013.376.
89. Inglis in Lin and Zegart 2019.25–26; Conti and Raymond 2017.45; Buchanan 2017.7, 110; Government of the United States, Office of the Under Secretary of Defence for Acquisition: Technology and Logistics 2017.4, 12; NATO Parliamentary Assembly, Science and Technology Committee 2019.5; Eilstrup-Sangiovanni 2018.
90. Matania and Tal-Shir 2020.286; Inglis in Lin and Zegart 2019.29; Long in Lin and Zegart 2019.118–119; Segal 2017.266; Eilstrup-Sangiovanni 2018; Harknett and Goldman 2016.86.
91. https://www.techopedia.com/.
92. Sanger 2018.72.
93. Former Commander of the NSA and Cyber Command, Adm. Michael Rogers, quoted by Cilluffo and Clark 2016.9. The 2015 DoD cyber strategy also rejects the notion that cyber inherently favors the offense or defense; Cilluffo and Clark 2016.4.
94. Buchanan 2017.53.
95. Libicki in Lin and Zegart 2019.142.
96. Perkovich and Levite 2017.194–195.
97. Buchanan 2017.65–67; Jasper 2017.18, 169–171.
98. Kehler in Lin and Zegart 2019.293–294; Healey 2019b.5.
99. Kehler in Lin and Zegart 2019.293–294; Perkovich and Levite 2017.193–194; Jasper 2017.18.

100. Government of the United States, White House 2017.13; Government of the United States, Department of Defense 2018.1–2; Government of the United States, Department of Defense 2015b.5–6; Government of the United States, Department of Defense, US Cyber Command 2018.6.
101. Government of the United Kingdom 2016.33; Wechsler 2018.63–64; Ali Craword, *Real Clear Defense*, January 14, 2019.
102. Clarke and Knake 2010.159.
103. Jasper 2017.112, 130; Buchanan 2017.54.
104. Perkovich and Levite 2017.49.
105. Cohen and Rotbart 2013.
106. Inglis in Lin and Zegart 2019.29; Long in Lin and Zegart 2019.118–119; Segal 2017.266; Matania and Tal-Shir 2020.286; Eilstrup-Sangiovanni 2018.
107. Conti and Raymond 2017.45, 266; Libicki in Lin and Zegart 2019.139–140, 142–143; Jasper 2017.116.
108. Siboni and Assaf 2016.
109. Lynn 2014; Chong 2014.
110. Jasper 2017.16.
111. Jasper 2017.20, 166, 174–175.
112. Harris 2014.204.
113. Jasper 2017.174, 183, 204.
114. Jasper 2017.178.
115. Jasper 2017.201–202.
116. Jasper 2017.20, 201; Harris 2014.105–106, 118.
117. Harris 2014.118–119, 171–172; Jasper 2017.204.
118. Harris 2014.118–119, 171–172; Jasper 2017.204.
119. Stacy Liberatore, *Daily Mail*, June 12, 2021.
120. Fanelli 2016.54–55.
121. Harknett and Goldman 2016.82, 85; Jervis 2016.66; Fanelli 2016.54, 60.
122. Government of the United States, Department of Defense 2018; US Government, Department of Defense, US Cyber Command June 2018.5–6; Harknett 2018.
123. Government of the United Kingdom 2016.25, 51.
124. Perkovich and Levite 2017.172.
125. Perkovich and Levite 2017.172.
126. Healey 2019b.30; Fanelli 2016.60, 62.
127. Interview, Eviatar Matania.
128. Harknett 2018; Nye 2016/2017.45.
129. Farrell and Glaser in Lin and Zegart 2019.60.
130. Even and Siman-Tov 2012.20.
131. Government of the United States, Department of Defense 2015; Demchak 2011; Demchak 2012b.
132. Singer and Friedman 2014.170–171.
133. Trobisch 2014.
134. Dana Pasquali, *DarkReading.com*, August 2, 2016; Trobisch 2014.
135. Inserra & Bucci 2014.
136. International Institute for Strategic Studies 2021.
137. David Sanger, *New York Times*, June 15, 2021; International Institute for Strategic Studies 2021.
138. Matania and Rappaport, Cybermania, 2021.1007.
139. International Institute for Strategic Studies 2021.
140. Matania and Rappaport, Cybermania, 2021.1007.
141. Interview, Eviatar Matania.
142. Cilluffo and Clark 2016.9.
143. Cilluffo and Clark 2016.9.
144. Cilluffo and Clark 2016.7, 10.
145. Laura Rosenberger, *Foreign Affairs*, 2020; Siman-Tov in Kuperwasser and Siman-Tov 2019.38–39.

146. Cilluffo and Clark 2016; Rid 2013; Gartzke 2013; Cohen and Levin 2014b; Libicki 2009; Cherry 2005; Weimann 2005; Kushner 2013.
147. Rid 2013.viii, xiv–xv, 1–3, 9, 13, 41.
148. Rovner 2019.
149. Cilluffo and Clark 2016.5–6.

Chapter 4

1. Barak Ravid, *Haaretz*, September 21, 2014; Rosenberg and Israel Defense Forces 2016; Amos Harel, *Haaretz*, August 30, 2018.
2. Graumann 2012.66; Eisenstadt and Pollock 2012; David Shamah, *Times of Israel*, July 9, 2014.
3. Ben-David 2011.57.
4. Tofi Stoler and Shahar Ilan, *CTech.com*, January 30, 2018.
5. Amir Bochbot, *Walla*, June 7, 2020.
6. Ben Zion Gad, *Jerusalem Post*, January 12, 2022; Amitai Ziv, *Haaretz.com*, September 21, 2020; Meir Obach, *Calcalist*, September 7, 2020.
7. Yaakov Lappin, *Jerusalem Post*, August 17, 2014; Yoav Limor, *Israel Hayom*, February 7, 2019.
8. TOI Staff, *Times of Israel*, April 15, 2015, and July 17, 2020; Mitch Ginsburg, *Times of Israel*, June 24, 2015; Ezra Kreiner and Joe Charlaff, *Jerusalem Post*, December 28, 2017; Simone Shemer, *NoCamels*, January 29, 2020.
9. Dan Goodin, *ARSTechnica*, January 26, 2016.
10. TOI Staff, *Times of Israel*, January 26, 2016; Danna Harman, *Haaretz*, January 26, 2016.
11. Amos Harel, *Haaretz*, May 20, 2020; Yonah Jeremy Bob, *Jerusalem Post*, May 28, 2020.
12. Fiona Willian, *9 News*, July 2, 2019; Statista Research Department, *Statista*, September 16, 2019.
13. Nor Dvori, *HaMadura HaMerkazi*, January 26, 2019; TOI Staff, *Times of Israel*, January 26, 2020.
14. Tzvi Joffre, *Jerusalem Post*, April 1, 2021.
15. Government of Israel; Prime Minister's Office, National Cyber Directorate 2019; https://block.org.il/news/caution-ransom-attack-in-front-of-you-the-accessibility-plugin-has-been-replaced-by-malicious-code/.
16. Amos Harel, *Haaretz*, July 9, 2017; Amos Harel, *Haaretz*, July 13, 2017; Yaniv Yakubobich, *Haaretz*, January 13, 2019.
17. Ben Caspit, *al-Monitor*, February 12, 2019; Shamir and Bachar 2019.10–11.
18. Netael Bendel, *Haaretz*, December 7, 2020.
19. See section on Iranian CNI attacks later in this chapter for sources.
20. Itam Elmadon, *N12*, January 21, 2021; Yoav Limor, *Israel Hayom*, February 7, 2019.
21. Yohav Zitun, *YNetnews.com*, May 8, 2017.
22. Yoav Limor, *Israel Hayom*, February 7, 2019.
23. Jordan Brunner, *The Tower.com*, August 2015.
24. Even and Siman-Tov 2012; Tofi Stoler and Shahar Ilan, *CTech.com*, January 30, 2018.
25. Jonathan Silber, *YNetnews.com*, January 26, 2012.
26. Daniel Cohen and Danielle Levin, *Forbes*, August 12, 2014; Siboni and Kronenfeld 2013.
27. Mohammed Herzallah, *Newsweek*, July 27, 2009.11; Anshel Pfeffer, *Haaretz*, December 10, 2009; Or Hirshoga and Nati Toker, *The Marker*, November 12, 2012; Olga Khazan, *Washington Post*, November 17, 2012; Michael Zippori, *CNN*, January 26, 2012; Stuart Winer, *Times of Israel*, August 17, 2014; Valeriano and Maness 2015.170–171; Armin Rosen, *Business Insider*, August 19, 2014.
28. Brian Bennett, *Times of Israel*, June 7, 2021; Yaakov Lapin, *Jerusalem Post*, January 8, 2018; Ari Soffer, *Arutz Sheva*, August 28, 2014; Mary-Ann Russon, *International Business Times*, July 18, 2014; Daniel Cohen and Danielle Levin, *Forbes*, August 12, 2014.
29. Tal Shachaf, *Ynet*, February 9, 2020; Anshel Pfeffer, *Haaretz*, June 15, 2009; Oded Yaron, *Haaretz*, February 16, 2015; Jacob, *Encyclopedia of Cyberwarfare*, 2017.220–22; Henning, *Encyclopedia of Cyber Warfare*, 2017.
30. Yona Jeremy Bob, *Jerusalem Post*, December 8, 2021; Yuval Mann and Gad Lior, *Ynet*, December 8, 2021.

31. Carr 2012.21–22.
32. Sue Surkes and Shoshana Solomon, *Times of Israel*, January 14, 2019; Rab Bar-Zik, *Haaretz,* February 9, 2020.
33. Ran Bar-Zik, *Haaretz*, December 10, 2020.
34. Yonah Jeremy Taub, *Jerusalem Post*, February 25, 2019; David Horovitz, *Times of Israel*, February 6, 2019; Shuker and Siboni 2019.27–28; Bergman, *Ynet*, July 31, 2018.
35. TOI Staff, *Times of Israel*, August 7, 2018; Shuker and Siboni 2019.38.
36. ClearSky Research Team, *ClearSky Cyber Security*, July 25, 2017.
37. Government of Israel; Prime Minister's Office, National Cyber Directorate 2020; Rapahel Kahan, *Calcalist*, December 14, 2020.
38. Kausch and Tabanksy 2018.8; Yonah Jeremy Taub, *Jerusalem Post,* February 25, 2019; Sam Jones, *Financial Times*, April 26, 2016; Ashish Kumar Sen, *Atlantic Council*, April 10, 2015.
39. Ben-Moshe 2022.
40. Sanger 2018.244, 260–262, 265.
41. Herb Canaan, *Jerusalem Post*, October 30, 2019.
42. Armin Rosen, *Business Insider*, July 28, 2014; James Vincent, *Independent*, July 29, 2014; Joe Miller, *BBC.com*, July 31, 2014; Danny Zaken, *Globes*, January 19, 2021.
43. *Jerusalem Post* Staff, *Jerusalem Post*, July 31, 2014.
44. TOI Staff, *Times of Israel*, October 28, 2013.
45. Yaniv Kobovich, *Haaretz*, November 19, 2019.
46. Amitai Zi, *Haaretz*, August 10, 2021; Patrick Howell O'Neill, *Technology Review.com*, August 10, 2021.
47. Ben-Moshe 2022.
48. Renan Bergman and Nicole Perlroth, *New York Times*, August 12, 2020; Yoav Zitun, *Ynet*, August 12, 2020.
49. https://www.pc.co.il/news/338803/.
50. Tal Shachaf, *Ynet*, February 9, 2020.
51. *Ynet*, November 8, 2021.
52. David Horowitz, *Times of Israel*, January 31, 2016; Cora Currier and Henrik Moltke, *The Intercept*, January 28, 2016.
53. Cora Currier and Henrik Moltke, *The Intercept*, January 28, 2016.
54. Amos Harel, *Haaretz*, August 20, 2018; TOI Staff, *Times of Israel*, January 29, 2016.
55. TOI Staff, *Times of Israel*, January 29, 2016.
56. Valeriano and Manness 2015.170.
57. Cohen and Rotbart 2013.113.
58. Yaakov Lapin, *Jerusalem Post*, January 8, 2018; Ari Soffer, *Arutz Sheva*, August 28, 2014; Mary-Ann Russon, *International Business Times*, July 18, 2014; Daniel Cohen and Danielle Levin, *Forbes*, August 12, 2014; Even and Siman-Tov 2012. 37; Mohammed Herzallah, *Newsweek*, July 27, 2009, 11; Stuart Winer, *The Times of Israel*, August 17, 2014; Siboni and Kronenfeld 2014.
59. Yoav Limor, *Israel Hayom*, February 7, 2019.
60. Oded Yaron, *Haaretz*, June 13, 2016; Nart Villeneuve, Thoufique Haq, and Ned Moran, *Fire Eye*, August 23, 2013; Pierluigi Paganini, *Security Affairs*, January 31, 2017; Clearsky Cybersecurity, June 2016; *Israel Hayom*, April 11, 2019.
61. Niv Elis, *Jerusalem Post*, February 17, 2015.
62. Tal Shahaf, *Ynet*, May 8, 2019.
63. Yoav Zitun, *YNetnews.com*, January 11, 2017.
64. Yaniv Kubovich, *Haaretz*, July 3, 2018; Amir Rapaport, *Israel Defense*, December 1, 2017; Tal Shahaf, *Globes: Israel's Business Arena*, July 18, 2018.
65. Yoav Zitu, *YNet*, July 14, 2019.
66. David Halbert, *New York Times*, February 16, 2020; Dov Liber, *Wall Street Journal*, February 16, 2020; Yaniv Kobovich, *Haaretz*, February 16, 2020.
67. Omer Benjakob, *Haaretz*, April 7, 2022.
68. *The Marker*, November 26, 2011.
69. Nir Dvori, *N12*, December 9, 2020; Tal Shahaf, *Ynet*, February 13, 2020.
70. Anshel Pfeffer, *Times of London*, October 22, 2020.

71. TOI Staff, *Times of Israel*, March 12, 2016; Hazem Balousha and William Booth, *Washington Post*, March 13, 2016.
72. AFP, *Times of Israel*, November 30, 2016.
73. Itamar Eichner, *YNetnews.com*, January 18, 2017.
74. Will Crisp and Suadad a-Salhy, *The Telegraph*, August 2, 2020.
75. Eyal Pinko, *Israel Defense*, March 30, 2021.
76. Oded Yaron, *Haaretz*, April 8, 2015.
77. Rid 2013.103.
78. Jeff Moskowitz, *Christian Science Monitor*, June 1, 2015.
79. TOI Staff, *Times of Israel*, June 14, 2015.
80. Ryan De Souza, *Hack Read*, February 21, 2016; Sagi Cohen, *YNetNews*, June 15, 2015.
81. Amichai Stein, *Kan Hadashot*, January 28, 2021; Tal Shachaf, *YNet*, January 28, 2021; Raphael Kahan, *Calcalist*, January 28, 2021; https://www.pc.co.il/news/331154/.
82. Emanuel Fabian, *Times of Israel*, June 29, 2022.
83. Anshel Pfeffer, *Haaretz*, June 15, 2009; Oded Yaron, *Haaretz*, February 16, 2015; Evan and Siman-Tov 2012; Jacob, *Encyclopedia of Cyberwarfare*. 2017.220–221.
84. Ron Ben-Yishai, *YNet*, July 24, 2021.
85. Gili Cohen, *Haaretz*, March 23, 2016.
86. Yonah Jeremy Bob, *Jerusalem Post*, March 23, 2016.
87. Yonah Jeremy Bob, *Jerusalem Post*, March 23, 2016.
88. Ron Ben-Yishai, *YNetnews.com*, March 23, 2016.
89. Kenney 2015.112, 117–119, 121.
90. Michael Margolit and Ran Boker, *YNetnews.com*, April 7, 2015; Jack Moore, *Newsweek*, April 7, 2015; Anonwatcher, *AnonHQ.com*, April 6, 2017; Israel Today Staff, *Israel Today*, April 16, 2016; Alexander J. Apfel, *YNetnews.com*, April 7, 2016; Institute for National Security Studies and the Cyber Security Forum Initiative 2014b; Jack Moore, *Newsweek*, April 7, 2015; Siboni et al. 2013.6, 7; Stuart Winer, *Times of Israel*, April 7, 2015; Adnan Abu Amer, *Al-Monitor*, July 29, 2015; Wang Wei, *Hacker News*, April 7, 2015; Brandon Stosh, *Freedom Hacker*, April 7, 2015; TOI Staff, *Times of Israel*, March 31, 2017; Mordechai Sones, *Israel National News*, March 26, 2017; Alexander J. Apfel, *YNetnews.com*, April 7, 2016; Daniel Smith, *Radware Blog*, April 25, 2017.
91. Baram 2017; Schaake 2020.30.
92. Siboni 2015.
93. INSS Insight 2014a.598.

Chapter 5

1. Anderson and Sadjadpour 2018.10–11; Siboni and Kronenfeld 2013.81–103; Kausch and Tabansky 2018.9; Siboni et al. 2020.22.
2. Sanger 2018.46–49; Segal 2017.5; Sam Jones, *Financial Times*, April 26, 2016; Siboni and Kronenfeld 2013.
3. Tabatabai 2020.12, 14.
4. Anderson and Sadjadpour 2018.13, 14, 31, 35–36, 52; ClearSky Research Team 2016; International Institute for Strategic Studies 2021; David Shamah, *Times of Israel*, August 13, 2015.
5. Siboni et al. 2020.22; Robert McMillan, *Wall Street Journal*, March 6, 2019; Sam Jones, *Financial Times*, April 26, 2016; Government of the United States, Director of National Intelligence 2021.14.
6. Sulmeyer 2017.38; David Rose, *The Mail*, February 17, 2018.
7. INSS Insight 2014a.561.
8. Micah Loudermilk, *Washington Institute for Near East Policy*, July 9, 2019.
9. Sam Jones, *Financial Times*, April 26, 2016.
10. Siboni et al. 2020.22; International Institute for Strategic Studies 2021.
11. Government of the United States, Congressional Research Service 2020; Brunner 2017.6–7; Siboni and Kronenfeld 2013.82,87–88; Çahmutoglu 2021.14–15.
12. Financial Tribune Staff, *Financial Tribune*, August 31, 2018.

13. Jasper 2017.41; Sam Jones, *Financial Times*, April 26, 2016; Dorothy Denning, *Navy Times*, January 24, 2020; Government of the United States, Congressional Research Service 2020; Anderson and Sadjadpour 2018.17; International Institute for Strategic Studies 2021; Tom Brewster, *The Guardian*, August 19, 2014; Sam Jones, *Financial Times*, April 26, 2016; Çahmutoglu 2021.15; Maryam Sinaiee, *Iran International*, November 17, 2020; Gordon Corera, *BBC News*, February 8, 2021.
14. Anderson and Sadjadpour 2018; Sam Jones, *Financial Times*, April 26, 2016.
15. Sam Jones, *Financial Times*, April 26, 2016; Sulmeyer 2017.39; Dorothy Denning, *Navy Times*, January 24, 2020; Anderson and Sadjadpour 2018.13.
16. Tabatabai 2020.8.
17. Jasper 2017.41; Kausch and Tabansky 2018.8; Micah Loudermilk, *Washington Institute for Near East Policy*, 2019; Siboni and Kronenfeld 2014.81–82; Anderson and Sadjadpour 2018.12; Tabatabai 2020.3, 8.
18. Micah Loudermilk, *Washington Institute for Near East Policy*, July 9, 2019; Sulmeyer 2017.34–35; Siboni and Kronenfeld 2014.81–103; International Institute for Strategic Studies 2020.536; Siboni et al. 2020.35.
19. Mahsa Alimardani, *Advox*, September 2, 2016.
20. Siboni and Kronenfeld 2014.81–103.
21. Jon Gambrelli, *AP*, January 28, 2018.
22. IFP Staff, *Iran Front Page*, May 28, 2020; Mahsa Alimardani, *Advox*, September 2, 2016.
23. Jon Gambrelli, *AP*, January 28, 2018; https://medialandscapes.org/country/iran/telecommunications/mobile-ownership#:~:text=Today%2C%20out%20of%20a%20population,is%20present%20in%20the%20country.
24. Lily Hay Newman, *Wired*, November 17, 2019; Carol Morello and Sissy Ryan, *Washington Post*, December 5, 2019; *Reuters*, December 23, 2019.
25. Isabel Debre, *AP*, May 20, 2022; Matt Burgess, *Wired*, September 23, 2022; David Cloud and Benoit Faucon, *Wall Street Journal*, September 25, 2022.
26. Jasper 2017.41; Kausch and Tabansky 2018.8; Micah Laudermilk, *Washington Institute for Near East Policy*, July 9, 2019; Siboni and Kronenfeld 2014.81–82; Anderson and Sadjadpour 2018.12; Tabatabai 2020.3, 7.
27. Tabatabai 2020.3, 6–8; Anderson and Sadjadpour 2018.42.
28. Cyber Threat Brief, *Flash Critic*, November 29, 2015.
29. John Hardy and Annie Fixler, *C4ISR*, February 8, 2021.
30. John Hardy and Annie Fixler, *C4ISR*, February 8, 2021; Setareh Behroozi, *Tehran Times*, June 24, 2019.
31. Omree Wechsler, *Council on Foreign Relations*, March 15, 2021; Morgan Demboski, *IronNet*, September 14, 2021; Ardavan Khoshnood, *Begin-Sadat Center for Strategic Studies*, March 4, 2021; John Hardy and Annie Fixler, *C4ISR*, February 8, 2021.
32. *Reuters*, October 21, 2019; Jack Corrigan, *NextGov*, October 23, 2019.
33. Faraz Fassih and Steven Lee Myers, *New York Times*, July 16, 2020, and March 29, 2021; *Reuters*, October 21, 2019; Eyal Pinko, *Israel Defense*, March 30, 2021; Jack Corrigan, *NextGov*, October 23, 2019; Golnaz Esfandiari, *Radio Free Europe, Radio Liberty*, September 4, 2020.
34. Sanger 2018.50; Micah Loudermilk, *Washington Institute for Near East Policy*, July 9, 2019.
35. Shimon Prokupecz and Tal Kopan, *CNN*, December 21, 2015; Dustin Volz and Jim Finkle, *Reuters*, March 24, 2016; Sanger 2018.47–48; Government of the United States, Director of National Intelligence 2021.14.
36. Sanger 2018.51–52; Reuters, *New York Times*, December 9, 2012; Sulmeyer 2017.37; Dorothy Denning, *Navy Times*, January 24, 2020; Government of the United States 2020.12; Siboni et al. 2020.22.
37. Segal 2017.151.
38. Siboni and Kronenfeld 2013.31; Siboni et al. 2020. 22; Tom Brewster, *The Guardian*, August 29, 2014; https://nbcnews.to/2uFfKi0.
39. Anderson and Sadjadpour 2018.40; Tabatabi 2020.17; Robert McMillan, *Wall Street Journal*, March 6, 2019; Micah Loudermilk, *Washington Institute for Near East Policy*, July 9, 2019; Nicole Perloth, *New York Times*, February 28, 2019; Raphael Satter, *AP*, December 13, 2018.
40. Yona Jeremy Bob, *Jerusalem Post*, July 27, 2021.

41. Dustin Volz, June 1, 2022.
42. Fatima Hussein and Frank Bajak, *AP*, September 9, 2022; Lila Hay Newman, *Wired*, August 4, 2022; David Gritten, *BBC News*, September 7, 2022.
43. Corey Dickstein, *Stars & Stripes*, October 4, 2019; Anderson and Sadjadpour 2018.31, 40; Robert McMillan, *Wall Street Journal*, March 6, 2019; Micah Loudermilk, *Washington Institute for Near East Policy*, July 9, 2019; Nicole Perloth, *New York Times*, February 28, 2019.
44. M. Dombrowski, *IronNet*, September 15, 2021.
45. Nicole Perloth, *New York Times*, February 28, 2019; Ewen MacAskill, *The Guardian*, October 13, 2017; Steven Erlanger, *New York Times*, June 24, 2017; Ken Dilian, *NBC*, February 28, 2019.
46. Rachel Weiner, *Washington Post*, September 17, 2020.
47. Ronen Bergman and Farnaz Fasshihi, *New York Times*, September 18, 2020.
48. M. Dombrowski, *IronNet*, September 15, 2021.
49. Tim Stickings, *The National News*, May 12, 2021; Ellen Nakashima and Spencer Hsu, *Washington Post*, March 27, 2019.
50. Cory Dickstein, *Stars & Stripes*, October 4, 2019; Ellen Nakashima and Spencer Hsu, *Washington Post*, March 27, 2019; Zak Doffman, *Forbes.com*, July 3, 2019; https://www.us-cert.gov/ncas/current-activity/2019/06/24/CISA-Statement-Iranian-Cybersecurity-Threats.
51. Rachel Weiner, *Washington Post*, September 17, 2020; Kristin Setera, *FBI*, September 17, 2021; Associated Press, reported in the *Washington Post*, October 28, 2020.
52. Gordon Corera, *BBC News*, February 8, 2021; M. Dombrowski, *IronNet*, September 15, 2021.
53. https://www.darkreading.com/vulnerabilities-threats/iran-linked-apt-cozies-up-enemies-trust-based-spy-game.
54. Jake Stubbs and Christopher Bing, *Reuters*, August 28, 2018.
55. Tabatabai 2020.3, 6–8, 18.
56. Itay Haiminis in Kuperwasser and Siman-Tov 2019.143; Tabatabai 2020.14; Ami Rojkes Dombe, *Israel Defense*, April 2, 2019; *Reuters*, May 6, 2020; Elaine Nakashima and Josh Dawsey, *Washington Post*, June 4, 2020; Craig Timberg et al., *Washington Post*, August 21, 2018; Daisuke Wakabayashi, *New York Times*, August 23, 2000; Craig Timberg and Tony Romm, *Washington Post*, July 25, 2019; Jay Greene, Tony Romm, and Ellen Nakashima, *Washington Post*, October 4, 2019.
57. Kate O'Flaherty, *Forbes*, October 9, 2020.
58. Tabatabai 2020.18, 20.
59. Julian Barnes and David Sanger, *New York Times*, October 21, 2020; Ellen Nakashima et al., *Washington Post*, October 21, 2020; Ellen Nakashima, Amy Gardner, and Aaron Davis, *Washington Post*, December 22, 2020; Tabatabai 2020.11, 15, 16; Government of the United States, National Intelligence Council 2021.5–7; Miles Parks, *NPR*, June 4, 2020; Brian Bennett, *Time*, June 7, 2021; David Sanger and Julian Barnes, *New York Times*, November 18, 2021; Phil Muncaster, *Infosecurity Magazine*, October 22, 2020; Lily Hay Newman, *Wired*, November 18, 2021.
60. Charles Hymas, *The Telegraph*, June 6, 2021; Stott 2021.
61. Clint Watts, former FBI agent, quoted in Brian Bennett, *Time*, June 7, 2021.
62. Amir Vahdat and Jon Gambrell, *AP*, May 22, 2020; Tamar Pileggie, *Times of Israel*, June 4, 2018; CNN Staff, *CNN*, December 15, 2000.
63. Stuart Winer and Marissa Newman, *Haaretz*, November 10, 2014.
64. Jerusalem Post Staff, *Jerusalem Post*, March 15, 2021; Amos Harel, *Haaretz*, April 16, 2010; Amos Harel, *Haaretz*, April 23, 2010; Amos Harel, *Haaretz*, July 24, 2013; Gili Cohen, *Haaretz*, March 31, April 2, 2015, and September 16, 2016; Yossi Yehoshua, *Yediot Aharonoth*, September 16, 2016.
65. Freilich 2018.154–160.
66. Freilich 2018.chapter 3.
67. David Shamah, *Times of Israel*, August 13, 2015; David Shamah, *Times of Israel*, October 28, 2012.
68. Yaakov Lappin, *Jerusalem Post* August 17, 2014.
69. Tom Brewster, *The Guardian*, August 29, 2014.

70. Sam Jones, *Financial Times*, April 26, 2016.
71. Yoav Limor, *Israel Hayom*, February 7, 2019.
72. Meir Orbach and Golab Hazani, *Calcalist*, December 13, 2020.
73. Achia Raabd, *Ynet* (Hebrew), May 19, 2020; Ynet staff, *YNet* (Hebrew), May 7, 2020; Amos Harel, *Haaretz*, May 20, 2020; Yonah Jeremy Bob, *Jerusalem Post*, May 28, 2020; Amitai Ziv, *The Marker* (Hebrew), June 1, 2020; Nir Dvori, *N12* (Hebrew), May 28, 2020; Staff, *Times of Israel*, May 19, 2020; Staff, *Jerusalem Post*, June 7, 2020; Amir Bochbot, *Walla*, June 7, 2020; https://bit.ly/34D3vET; Tal Shachaf, *YNet*, February 17, 2021; Government of Israel, Prime Minister's Office, National Cyber Directorate 2021.
74. Yonah Jeremy Bob, *Jerusalem Post*, May 28, 2020, and December 10, 2020.
75. Staff, *Times of Israel*, July 17, 2020; Amos Harel, *Haaretz*, September 21, 2022.
76. Staff, *Ynet* May 21, 2020; Ron Bar-Zik, *Haaretz*, May 21, 2020; Government of Israel, Prime Minister's Office, National Cyber Directorate 2021.
77. Yoav Limor, *Israel Hayom*, June 11, 2020.
78. Morgan Dombowshi, *IronNet*, September 15, 2021; Yuval Mann, *YNet*, November 10, 2021.
79. Morgan Dombowshi, *IronNet*, September 15, 2021.
80. Amos Harel, *Haaretz*, September 21, 2022; Tzvi Joffre, *Jerusalem Post*, October 13, 2021; Tal Shachaf, *YNet*, October 13, 2021; *Times of Israel staff*, October 18, 2021; http://hy.health.gov.il/eng/?CategoryID=23&ArticleID=1082; https://www.ifi.today/hitech/1617-The-cyber-ransom-attack-on-Hillel-Yaffe-hospital-Experts-work-on-rehabilitating-the-systems.html; https://cyberintelmag.com/attacks-data-breaches/alleged-chinese-hackers-behind-attacks-on-10-israeli-hospitals/.
81. Rafael Kahan, *Calcalist*, February 1, 2022; Genia Wilenski, *The Marker*, January 31, 2022; Nevo Trebelsi, *Globes*, January 31, 2022.
82. Amos Harel, *Haaretz*, March 15, 2022; Yaniv Kobovich and Oded Yaon, *Haaretz*, March 14, 2022; Yaniv Halperin, *Anashim Umachshevim*, March 14, 2022; Yaron Avraham and Nir Dvori, *N12*, March 14, 2022; Raphael Kahan, *Calcalist*, March 14, 2022; Stav Namer et al, *Maariv*, March 14, 2022; Daniel Salame, *YNet*, March 14, 2022.
83. Oded Yaron, *Haaretz*, July 10, 2022; *Times of Israel staff*, July 4, 2022; Luke Tress, *Times of Israel*, August 17, 2022.
84. https://13news.co.il/item/news/politics/security/iran-hackers-1162861/.
85. Ellen Nakashima, *Washington Post*, May 29, 2014; Nicole Perlroth, *New York Times*, May 19, 2014; Mandiant Corporation 2014.8–9; Nicole Perlroth, *New York Times*, May 19, 2014; Stephen Ward, *Insight Partners*, May 28, 2014; Pierluigi Paganini, *InfoSec*, February 20, 2017.
86. Minerva Labs, *Minerva Labs LTD and ClearSky Cyber Security*, November 23, 2015.
87. Government of the United States, United States Department of Justice 2018.
88. Anthony Cuthbertson, *The Independent*, August 24, 2018.
89. TOI Staff, *Times of Israel*, June 14, 2015.
90. ClearSky Cyber Security 2015.
91. Clearsky Research Team, *Clearsky.com*, September 1, 2015.
92. Tamar Pileggi, *Times of Israel*, August 10, 2015; David Shamah, *Times of Israel*, August 13, 2015.
93. ClearSky Cyber Security 2017.
94. Tamar Pileggi, *Times of Israel*, April 26, 2017; Gwen Ackerman and Alisa Odenheimer, *Bloomberg*, April 26, 2017; Anshel Pfeiffer, *Haaretz*, April 27, 2017.
95. Clearsky Research Team, *Clearsky.com*, January 25, 2017.
96. TOI Staff, *Times of Israel*, January 30, 2018.
97. NoCamels, February 1, 2018.
98. https://13news.co.il/item/news/politics/security/iran-hackers-1162861/.
99. Yoav Zitun, *YNet*, July 24, 2019.
100. Yaniv Kubovich, *Haaretz*, April 12, 2021.
101. Zev Stub, *Jerusalem Post*, October 6, 2021.
102. Yoav Zitun, *Ynet*, January 12, 2022; Jeffrey Hellers, *Reuters*, January 12, 2022; Anna Ahronheim, *Jerusalem Post*, January 12, 2021; Amos Harel, *Haaretz*, January 12, 2021.
103. Amos Harel, *Haaretz*, May 2, 2022; Yoav Zitun, *YNet*, May 2, 2022.
104. Morgan Dombowshi, *IronNet*, September 15, 2021.

105. Roi Dahan, *YNet*, June 14, 2022; Oded Yaron, *Haaretz*, June 14, 2022.
106. Morgan Dombowshi, *IronNet*, September 15, 2021; Yuval Mann, *YNet*, November 10, 2021.
107. Tzvi Joffre, *Jerusalem Post*, May 19, 2022.
108. Tabatabai 2020.15–19.
109. TOI Staff, *Times of Israel*, September 6 and November 30, 2018; Jake Stubbs and Christopher Bing, *Reuters*, August 28, 2018.
110. JPost.com Staff, *Jerusalem Post*, July 4, 2014; Institute for National Security Studies and the Cyber Security Forum Initiative 2014b; Siboni and Kronenfeld 2014; Kayla Ruble, *Vice*, July 17, 2014; Mohammad Herzallah, *Newsweek*, July 27, 2009; TOI Staff, *Times of Israel*, January 30, 2018.
111. TOI Staff, *Times of Israel*, September 6 and November 30, 2018.
112. Roi Rubenstein, *Ynet.com*, January 31, 2019; Shamir and Bachar 2019.12.
113. Scott Shane and Ronan Bergman, *New York Times*, May 14, 2019.
114. Sheera Frenkel, *New York Times*, June 30, 2021; Omer Benjakob, *Haaretz*, April 21, 2021.
115. Tal Shachaf and Nina Fuchs, *Ynet*, October 26, 2021; Tal Shachaf, *Ynet*, October 26, 2021.
116. Itamar Eichner and Yuval Mann, *YNet*, September 4, 2022.
117. Itamar Eichner, *YNet*, June 20, 2022.
118. Omer Benjakob and Oded Yaron, *Haaretz*, July 13, 2022.
119. Yoav Zitun, *YNet*, May 2, 2022.
120. Meir Orbach, *Calcalist*, June 14, 2020.
121. Meir Orbach, *Calcalist*, September 7, 2020; Amitai Ziv, *Haaretz*, September 21, 2020.
122. Omer Benjakob, *Haaretz*, October 19, 2020.
123. Omer Benjakob, *Haaretz*, December 9, 2020; Hagay Cohen, *Jerusalem Post*, November 12, 2020; Meir Orbach, *Algemeiner*, November 15, 2020.
124. Bernard Brode, *Times of Israel*, December 18, 2020.
125. Omer Benjakob, *Haaretz*, December 9, 2020; Oded Yaron, *Haaretz*, December 9, 2020; Yuval Mann, *YNet*, December 4, 2020; Nina Fox, *Ynet*, December 5, 2020; Uri Berkowitz, *Globes*, December 5, 2020; Amitai Ziv, *The Marker*, December 6, 23, and 31, 2020; Sami Peretz, *The Marker*, December 6, 2020; Tal Shachaf, *Ynet*, December 15, 2020; Tal Shachaf, *Ynet*, March 13, 2021.
126. Tal Shachaf, *Ynet*, December 13 and 15, 2020; Raphael Kahan, *Calcalist*, December 13, 2020; Meir Orbach and Golan Hazani, *Calcalist*, December 13, 2020.
127. Tal Shachaf, *YNet*, December 13, 15, and 17, 2020; Raphael Kahan, *Calcalist*, December 13, 2020; Amitai Ziv, *Haaretz*, December 13 and 31, 2020; Tal Schneider, *YNet*, December 20, 2020.
128. Tal Schneider, *YNet*, December 20, 2020; Yonah Jeremy Bob, *Jerusalem Post*, December 20, 2020; Omer Benjakob, *Haaretz*, December 20, 2020.
129. Tal Shachaf, *YNet*, March 13, 2021; Amitai Ziv, *Haaretz*, May 5, 2021.
130. Adir Yanko, Tak Shachaf, and Hadar Gil-Ad, *Ynet*, November 1, 2021; Farnaz Fassihi and Ronen Bergman, *New York Times*, November 27, 2021.
131. Tom Bateman, *BBC*, February 3, 2022.
132. Interview, Eviatar Matania; Amos Haaretz, *Haaretz*, September 25, 2022.
133. AFP, *i24News*, February 5, 2019.

Chapter 6

1. Kleiman 1990.53.
2. http://www.pitgam.net/data/%5B%D7%9E%D7%A0%D7%97%D7%9D+%D7%91%D7%92%D7%99%D7%9F%5D/1/1/0/.
3. Sima Kadmon, *Yediot Aharonot*, weekend magazine, November 18, 2006.
4. Peter Hirschberg, *Haaretz*, November 14, 2006.
5. Freilich, 2012.12; Dror 2011.13, 16; Brun 2008.4–15.
6. Freilich 2012.12.
7. Yaniv 1987.18–19; Ben-Israel 2013.59–60.
8. Freilich 2012.12; Maoz 2006.8; Horowitz in Yaniv 1993.32; Heller 2000.10; Adamsky 2010.112; Inbar 1990.165.

9. Dror 2011.18.
10. Dror 2011.4, 14.
11. Cohen 1991.28, 30.
12. Freilich 2012.54–55.
13. Handel 1973.1; Ben-Horin and Posen 1981.26; Maoz 2006.9; Yariv 1980.3–12, 6; Levite 1989.35; Bar-Joseph 2000.99–114, 100.
14. Shelah 2003.30; Yariv 1980.3–12; Gelber 2014.1.
15. Kober 2009.1, 3, 36; Feldman and Toukan 1997.10.
16. Kober 2009.1, 3, 36; Kober 1995.152.
17. Tal 1996.62–63.
18. Pedatzur in Bar-Tal et al. 1998.144; Ben-Horin and Posen 1981.13.
19. Horowitz in Yaniv 1993.16–18; Pedatzur in Bar-Tal et al. 1998.141, 147–148; Ben-Israel 2013.40; Ben-Horin and Posen 1981.10; Maoz 2006.13; Bar-Joseph 2004/2005.137–156; Ben-Dor in Bar-Tal et al. 1998.120.
20. Inbar 2008.86; Ben-Israel 2013.82; Maoz 2006.8, 15; Heller 2000.15.
21. Freilich 2018.294–308.
22. Tal 1996.62–63; Levite 1989.35; Feldman and Toukan 1997.8.
23. Baram and Ben-Israel 2018; Baram 2017.1.
24. Levite 1989.47.
25. Freilich 2018.166–174.
26. Heller 2000.13; Ben-Dor in Bar-Tal et al. 1998.114–115; Feldman and Toukan 1997.9–10.
27. Bar-Joseph 2004/2005.137–156.141; Bar-Joseph 2005.10–19.13; Feldman and Toukan 1997.9; Heller 2000.11; Levite 1989.39; Kober 1995.156–158; Adamsky 2010.112.
28. https://bit.ly/3M0utue.
29. Freilich 2018.185–186, 199.
30. Amos Harel, *Haaretz*, June 7, 2013; Aluf Benn, *Haaretz*, January 12, 2013; www.nrg.co.il/online/1/ART2/524/169.html.
31. Ganor 2005.27–28, 288–290; Catignani 2008.48.
32. Ganor 2005.chapters 4–5; Jones and Catignani 2010.68; Rodman 2013.3, 11.
33. Freilich 2018.209–210.
34. Byman 2011.4.
35. Ben-Israel 2013.120; Rubin 2007.18; Barbara Opall-Rome, *Defense News*, October 27, 2013; Dan Williams, *Reuters*, January 29, 2014.
36. Rubin 2012.5–6; Amos Harel, *Haaretz*, July 26, 2011; Shafir in Brom 2012.35–36; Kam in Brom 2012.15.
37. Chorev, 2015.25, 28, 33; Shamir and Hecht, 2014.88–89.
38. Inbar and Shamir 2013.12–13; Brom and Kurtz 2014.114; Sobelman 2016.17.
39. Amos Harel 2016.46; Ofer Shelah, Herzlia Conference, June 16, 2016; Reuven Pedatzur, *Haaretz*, October 30, 2012; Amos Harel and Avi Issacharoff, *Haaretz*, November 24, 2012; Amos Harel, *Haaretz*, August 4 and August 29, 2014; Even and Michael in Elran et al. 2016a.48; HaCohen in Elran et al. 2016a.101; Meir Elran and Carmit Pedan, *Israel News*, September–October 2016.22–22.
40. Aluf Benn, *Haaretz*, December 21, 2008.
41. Aluf Benn, *Haaretz*, December 21, 2008.
42. Ari Shavit interview with "The Decision Maker," *Haaretz*, August 10, 2012.
43. Except where specifically stated otherwise, the section on Israel's nuclear strategy is based on Freilich 2018.chapter 8.
44. Amos Harel, *Haaretz*, September 3 and October 18, 2013.
45. Jerusalem Post Staff, *Jerusalem Post*, August 7, 2015; www.*Haaretz*.com/israel-news/israel-s-mossad-trained-assassins-of-iran-nuclear-scientists-report-says-1.411945; www.theguardian.com/world/julian-borger-global-security-blog/2012/jul/11/israel-iran-nuclear-assassinations; www.israeltoday.co.il/NewsItem/tabid/178/nid/23644/Default.aspx; www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.
46. Levite 2010.160.

47. Ambassador Jeremy Issacharoff in Landau and Bermant 2014.196–197; Ambassador Eytan Bentsur, Director General MFA, Statement Before the Conference on Disarmament, Geneva, September 4, 1997; Feldman in Feldman and Toukan 1997.26; Bar 2008.150.
48. Landau 2013.3; Levite 2010.159, 161; Ambassador Jeremy Issacharoff in Landau and Bermant 2014.197; Brom in Blechman 2011.50; Feldman in Feldman and Toukan 1997.17, 26.
49. Ambassador Jeremy Issacharoff in Landau and Bermant 2014.196–197; Ambassador Eytan Bentsur, Director General, Statement Before the Conference on Disarmament, Geneva, September 4, 1997; Levite 2010.160; Landau and Stein in Foradori and Malin 2013.23–24.
50. Shapir in Bar-Joseph 2001.156; Cohen et al. 1998.41–42.
51. Except where stated otherwise, the section on national security decision-making in Israel draws on Freilich 2006; Freilich 2012; Freilich 2013; Freilich 2015; and Freilich in Cohen and Klieman 2019.
52. See Freilich 2012.
53. Freilich 2018.199.

Chapter 7

1. Adamsky 2017.114; Baram 2017.6; Tabansky and Ben-Israel 2015.31, 35.
2. Tabansky and Ben-Israel 2015.33; Housen-Couriel 2017.6; Baram 2013.28, 38; Ravid 2011; Adamsky 2017.114.
3. Goldschmidt 2017.3; Government of Israel, Prime Minister's Office, National Cyber Directorate 2018.
4. Ravid 2011; Adamsky 2017.114; Frei 2020.
5. Baram 2013.29, 36; Siboni 2013.8; Adamsky 2017.117; Tabansky 2013.8, 38; Tabansky and Ben-Israel 2015.35–38; Housen-Couriel 2017.11.
6. Tabansky and Ben-Israel 2015.37–38.
7. Tabansky and Ben-Israel 2015.37–38; Frei 2020.
8. Tabansky and Ben-Israel 2015.35–38; Frei 2020.
9. Tabansky and Ben-Israel 2015.39–40; Tabansky 2020.2; Frei 2020; Baram 2013.29, 36; Siboni 2013.8; Adamsky 2017.117; Tabansky 2013.8, 38; Housen-Couriel 2017.8, 11.
10. Matania and Rappaport, Cybermania, 2021.35, 40.
11. Isaac Ben-Israel, *Israel Forbes*, June 28, 2021; Tabansky and Ben-Israel 2015.43–47; Tabansky 2020.2; David Fulghum, *Aviation Week and Space Technology*, June 25, 2012; Ram Levi, *IsraelDefense*, December 16, 2011; Adamsky 2017.115.
12. Housen-Couiel 2017.8; Tabansky 2020.3; Government of Israel, Prime Minister's Office 2011.
13. Government of Israel, Prime Minister's Office 2011; Tabansky and Ben-Israel 2015.43–47, 49–54; Frei 2020; David Fulghum, *Aviation Week and Space Technology*, June 25, 2012; Ram Levi, *IsraelDefense*, December 16, 2011; Adamsky 2017.115.
14. Raska 2015; Tabansky and Ben-Israel 2015.55–57; Yonah Jeremy Bob, *Jerusalem Post*, August 25, 2018; Matania and Rappaport, Cybermania, 2021.529–533, 537.
15. Government of Israel, Cabinet Secretariat 2015a.
16. Government of Israel, Cabinet Secretariat 2015a.
17. Yossi Melman, *Maariv*, August 12, 2017.
18. Staff, *IsraelDefense*, January 29, 2019; Shoshanna Solomon, *Times of Israel*, June 25, 2018; Tabansky and Ben-Israel 2015.58–59.
19. Matania and Rappaport, Cybermania, 2021.537–563; Interviews, Ronen Korman and senior official #16.
20. Government of Israel, Cabinet Secretariat 2015b; Tabansky and Ben-Israel, 2015.58–59.
21. Interview, senior official #6.
22. Chachko 2020.5.
23. Adamsky 2017.120.
24. Goldschmidt 2017.3–5; Government of Israel, Prime Minister's Office, National Cyber Directorate 2018.7.
25. Government of Israel, Prime Minister's Office, National Cyber Directorate 2020; Government of Israel, Prime Minister's Office, National Cyber Directorate 2017c.25; Dan Arkin, *Israel Defense*, May 27, 2018; *Israel Defense*, April 3, 2017; *Israel Defense*, March 22, 2017.

26. Lecture, Prof. Eviatar Matania, Tel Aviv University, December 3, 2018.
27. Itai Green, *Times of Israel*, June 5, 2019; Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2017; Government of Israel, Prime Minister's Office, National Cyber Directorate 2017b, a brief summary of the strategy is available in English; Frei 2020.
28. Interview, senior official #14; Interview, senior official #18.
29. Interview, Eviatar Matania; Matania and Rappaport, Cybermania, 2021.
30. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2017.8.
31. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018.
32. Interview, senior official #14.
33. Interview, Eviatar Matania.
34. Except where specified otherwise, the following section is summarized from Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2017.
35. Matania et al. 2016.81–82.
36. Interview, Eviatar Matania.
37. Matania et al. 2016. 79–80; Matania and Rappaport, Cybermania, 2021.311–317; Barbara Opall-Rome, *DefenseNews*, July 11, 2016.
38. www.defensenews.com/story/defense/policy-budget/leaders/interviews/2016/07/11/israel-cybersecurity-directorate-matania/86445128.
39. Frei 2020; Matania et al. 2016.81–82; Matania and Rappaport, Cybermania, 2021.311–317.
40. Editorial, *Haaretz*, December 14, 2020; Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020.
41. State of Israel, Prime Minister's Office, National Cyber Directorate 2017c; Yossi Melman, *Maariv*, August 12, 2017; Amitay Ziv, *The Marker*, August 29, 2018; Yonah Jeremy Bob, *Jerusalem Post*, August 25, 2018.
42. Government of Israel, Prime Minister's Office, National Cyber Directorate 2017a; Government of Israel, Prime Minister's Office, National Cyber Directorate 2017d; Government of Israel, Prime Minister's Office, National Cyber Directorate 2018.
43. Government of Israel, Prime Minister's Office, National Cyber Directorate 2017a.
44. International Institute for Strategic Studies 2021.
45. Government of Israel, Prime Minister's Office, National Cyber Directorate 2018.
46. Government of Israel, Prime Minister's Office, National Cyber Directorate 2015.
47. Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020.
48. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016; Dan Arkin, *Israel Defense*, May 27, 2018; https://cert.gov.il/CERT-IL/SiteAssets/RFC2350.pdf; Shoshana Solomon, *Times of Israel*, July 2, 2017; Yaakov Lappin, *Jerusalem Post*, April 7, 2013; Government of Israel, Prime Minister's Office, National Cyber Directorate 2017.13.
49. Goldschmidt 2017.7; Yaakov Lappin, *Jerusalem Post*, April 7, 2013; Government of Israel, Prime Minister's Office, National Cyber Directorate 2017.13; Shabtai 2017; Sivan Aizescu, *Haaretz*, 2014; Government of Israel, Supervisor of Banks, 2015; Irit Avissar, *Globes*, July 21, 2014.
50. Dan Arkin, *Israel Defense*, May 27, 2018.
51. John Leyden, *The Register*, June 21, 2018; Soshanna Solomon, *Times of Israel*, February 1, 2017.
52. Yakkov Lappin, *Jerusalem Post*, November 19, 2010.
53. Yonah Jeremy Bob, *Jerusalem Post*, June 27, 2019.
54. Government of Israel, Prime Minister's Office, National Cyber Directorate 2020.
55. Viva Sarah Press, *Nocamels*, January 29, 2017; *Israel Defense*, January 29, 2019.
56. Douglas Karr, *Martech*, January 2, 2021.
57. Ran Bar-Zik, *Haaretz*, July 8, 2019.
58. Matania and Rappaport, Cybermania, 2021.1004; Government of Israel, State Comptroller 2022b.
59. Shuker and Siboni 2019.35–36; David Horovitz, *Times of Israel*, February 6, 2019.
60. Shuker and Siboni 2019.34–36; Amos Harel, *Haaretz*, July 13, 2017.
61. Shuker and Siboni 2019.34–36; Amos Harel, *Haaretz*, July 13, 2017.
62. Government of Israel, State Comptroller 2022b.

63. Attila Shomfalvi, *YNET*, October 16, 2021.
64. Amitai Ziv, *The Marker*, July 24 and November 5, 2019, January 23, 2020, and April 4, 2021.
65. Valeriano and Maness 2012.146; Shiryn Ghermezian, *Algemeiner*, April 10, 2014.
66. Stuart Winer, *Times of Israel*, April 7, 2015; Adnan Abu Amer, *Al-Monitor*, July 29, 2015; Institute for National Security Studies 2016; Brandon Stosh, *Freedom Hacker*, April 7, 2015.
67. TOI Staff, *Times of Israel*, June 23, 2020.
68. Soshanna Solomon, *Times of Israel*, February 1, 2017; Government of Israel; Prime Minister's Office, National Cyber Directorate 2020; Matania and Rappaport, Cybermania, 2021.633–637.
69. Dan Williams, *Reuters*, February 18, 2019.
70. Government of Israel, Prime Minister's Office, National Cyber Directorate 2020.
71. Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020; Joshua Shuman, *Jerusalem Post*, December 15, 2020.
72. TOI Staff, *Times of Israel*, June 2, 2015.
73. Yoav Zitun, *YNet*, January 25, 2012.
74. Yaniv Kobovich, *Haaretz*, October 31, 2021.
75. https://www.gov.il/he/departments/news/press_19022019.
76. https://www.gov.il/he/departments/news/press_19022019; http://bit.ly/2Ni9OWD.
77. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018; Chachko 2020.4–5.
78. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018; Interview, official #18.
79. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018; Interview, official #18.
80. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018.
81. Government of Israel, Prime Minister's Office, the National Cyber Security Authority 2018.
82. Shoshana Solomon, *Times of Israel*, June 25, 2018, Housen-Couriel 2018; https://www.gov.il/he/departments/news/cyberlawpublic.
83. Gili Cohen and Amos Harel, *Haaretz*, April 24, 2000; Yossi Melman, *Maariv*, August 12, 2017.
84. https://www.law.co.il/media/computer-law/cyber_defense_bill_draft_version2_2021.pdf; Housen-Couriel et al. 2021; Zohar Rosenberg, *Calcalist*, February 28 and March 1, 2021.
85. Zohar Rosenberg, *Calcalist*, February 28, 2021.
86. Housen-Couriel et al. 2021; Zohar Rosenberg, *Calcalist*, February 28 and March 1, 2021.
87. Government of Israel, State Comptroller 2016.
88. Government of Israel, Knesset, Foreign and Defense Affairs Committee, Subcommittee on Cyber-Defense 2016.
89. Government of Israel, State Comptroller 2019; Government of Israel, State Comptroller 2022a.
90. Interviews, senior officials #14 and #19.
91. Interviews, senior officials #14 and #19.
92. Interview, senior official #19.
93. Interview, Eviatar Matania.
94. Interview, senior officials #20 and 21.
95. Interview, senior official #19 and academic source.
96. Interview, senior official #21, senior official 22 and academic source.
97. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016; "Israel Sets Global Standard for Cyber Security," October 7, 2014, Ben-Gurion University.

Chapter 8

1. International Institute for Strategic Studies 2021.
2. Adamsky 2010.6; Adamsky 2019.1–2.
3. Taylor 2016.217, 220, 229–230.
4. International Institute for Strategic Studies 2021.6.
5. Housen-Couriel 2017.14.
6. Razin 2018.108; Tabansky and Ben-Israel.18; Frei 2020.

7. http://nocamels.com/2017/01/bloomberg-innovation-index-israel-tenth/; http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf.
8. Amir Mizroch, *Forbes*, May 7, 2019; http://innovationisrael-en.mag.calltext.co.il/article/69/1141.
9. Government of Israel, Israel Innovation Authority 2021.8.
10. Abigail Klein Lachman, *Israel 21C*, October 26, 2020; INCD Annual Report 2020; Baram and Ben-Israel, The Academic Reserve: Israel's Fast Track to High-Tech Success 2018; Taylor 2016.146.
11. http://innovationisrael-en.mag.calltext.co.il/article/69/1141; https://www.visualcapitalist.com/world-most-innovative-economies/; NoCamel's Team, February 3, 2021.
12. http://nocamels.com/2017/01/bloomberg-innovation-index-israel-tenth/; http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf; Taylor 2016.146.
13. Government of Israel, Israel Innovation Authority 2021.18; http://innovationisrael-en.mag.calltext.co.il/article/69/1141.
14. Eytan Halon, *Jerusalem Post*, August 22, 2019.
15. Shoshana Solomon, *Times of Israel*, July 18, 2019.
16. Nechemia Strassler, *Haaretz*, August 8, 2017; Amitai Ziv, *The Marker*, June 23, 2019.
17. Zach Cutler, *Entrepreneur*, April 23, 2015; *Israel Defense*, May 20, 2020.
18. Steinherz 2014; Amitai Ziv 2014, *Economist*, August 1, 2015; Amitai Ziv, *The Marker*, June 23, 2019, and January 22, 2020; Jordan Brunner, *The Tower*, August 2015.
19. https://i-hls.com/he/archives/82615.
20. http://legalinsurrection.com/2016/06/us-israel-sign-cyberdefense-agreement/; https://www.forbes.com/sites/elizabethmacbride/2016/07/18/five-lessons-on-cybersecurity-from-an-israeli-general/#616d36a74fd1.
21. Ricky Ben-David, *Times of Israel*, January 20, 2022.
22. NIV ELIS, *inShare* February 23, 2014; Adamsky 2017.119; https://www.bloomberg.com/news/articles/2017-04-26/israeli-official-says-first-wave-of-cyber hack-was-thwarted.
23. Government of Israel, Prime Minister's Office, National Cyber Directorate 2020; Matania and Rappaport, Cybermania, 2021.57.
24. http://www.readitnow.co.il/news; Richet 2015.293; Ellen Nakashima and Ruth Eglash, *Washington Post*, May 14, 2016; Erad Atzmon Shmayer and Amitai Ziv, *The Marker*, July 11, 2019.
25. http://www.mod.gov.il/Society_Economy/articles/Pages/10.2.16.aspx.
26. Viva Sarah Press, *Israel21c.org*, August 3, 2015.
27. International Institute for Strategic Studies 2021.
28. Interview, Isaac Ben-Israel.
29. Interviews, officials #19 and #20.
30. Adamsky 2017.118.
31. Matania and Rapppaport, Cybermania, 2021.375–387.
32. Adamsky2017.118; Amitai Ziv, *The Marker*, July 15, 2019.
33. http://economy.gov.il/English/Pages/default.aspx;http://economy.gov.il/English/About/Pages/About.aspx; http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokekidma131112.aspx; https://innovationisrael.org.il/en/sites/default/files/2018-19_Innovation_Report.pdf; https://innovationisrael.org.il/en/contentpage/innovation-israel; https://www.gov.il/he/departments/policies/2014_dec2092; https://rio.jrc.ec.europa.eu/en/library/rio-country-report-israel-2015; https://www.arnon.co.il/sites/default/files/files_from_old/Client%20Update%20-%20OCS%20-%20Amendment%207%20to%20R%26D%20Law%20%28YA-10.2015%29_0.pdf; https://www.rcip.co.il/en/article/on-the-establishment-of-a-national-authority-for-technological-innovation-amendments-to-the-law-for-the-promotion-of-industrial-research-and-development/; https://www.law.co.il/en/news/2016/01/05/israel-r-d-law-establishes-new-authority-for-innovation/; https://mof.gov.il/chiefecon/internationalconnections/oecd/oecd%20enterp.pdf.
34. http://www.matimop.org.il/programs.html; Baram 2013.34.

35. Ricky Ben David, *Times of Israel*, November 17, 2021; http://tlabs.bgu.ac.il/index.php/the-news/137-deutsche-telekom-innovation-laboratories-at-bgu-dedicates-expanded-offices; https://www.research.ibm.com/haifa/ccoe/; https://www-03.ibm.com/press/us/en/pressrelease/43075.wss; http://support.huji.ac.il/news-events/news/New-Joint-Israeli-2FGerman-Center-to-Revolutionize-Cybersecurity/.
36. Tabansky 2020; Taylor 2016.144; Omer Keilaf, *Forbes*, July 3, 2020.
37. Adamsky 2017.123; Omer Keilaf, *Forbes*, July 3, 2020; Swed and Butler 2013; https://www.wsj.com/articles/israeli-army-builds-a-desert-outposttech-firms-follow-1433525715; https://www.forbes.com/sites/elizabethmacbride/2016/07/18/five-lessons-on-cybersecurity-from-an-israeli-general/#616d36a74fd1.
38. Sophie Shulman, *Calcalist*, January 8, 2021; https://81amit.org.il/about/.
39. NoCamels Team, "Israel's Defense Ministry Launches Innovation Center for Cutting Edge Security Tech," August 12 2019; https://finder.startupnationcentral.org/program_page/innofense; https://accelerator.i-hls.com/.
40. Sagy Cohen, *The Marker*, September 26, 2019.
41. Shoshana Solomon, *Times of Israel*, May 22, 2019.
42. Interview, Tom Ahi Dror.
43. Interview, Tom Ahi Dror.
44. Interview, Sagy Bar.
45. Interview, Tom Ahi Dror.
46. Shaul Amsterdamsky, *Kan.org*, April 15, 2021; Government of Israel, Israel Innovation Authority 2021.10.
47. Interview, Tom Ahi Dror.
48. Interview, Tom Ahi Dror.
49. http://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission.
50. http://cyber.org.il/.
51. https://he.wikipedia.org/wiki/%D7%9E%D7%92%D7%A9%D7%99%D7%9E%D7%99%D7%9D_-_%D7%AA%D7%95%D7%9B%D7%A0%D7%99%D7%AA_%D7%94%D7%A1%D7%99%D7%99%D7%91%D7%A8_%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99%D7%AA; http://www.rashi.org.il/—c1pcq; Isaac Ben-Israel, Meeting at the Belfer Center, Kennedy School of Government, September 14, 2017.
52. Interview, Sagy Bar; http://cyber.org.il/; http://www.timesofisrael.com/in-israel-teaching-kids-cyber skills-is-a-national-mission/; www.csmonitor.com/World/Middle-East/2013/0609/Israel-accelerates-cybersecurity-know-how-as-early-as-10th-grade; Tabansky and Ben-Israel 2015.1, 27; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016; http://www.magshimim.cyber.org.il/; Yossi Yehoshua and Reuven Weiss, *YNet*, December 6, 2020.
53. Interview, Sagy Bar; Interview, Tom Ahi Dror; Yossi Yehoshua and Reuven Weiss, *YNet*, December 6, 2020; Frei 2020; www.csmonitor.com/World/Middle-East/2013/0609/Israel-accelerates-cybersecurity-know-how-as-early-as-10th-grade.
54. Yossi Yehoshua, *YNet*, July 13, 2022.
55. Interview, Tom Ahi Dror.
56. Interview, Sagy Bar; Sivan Greenbaum-Eshed, *The Marker*, Cyber Supplement, June 2018; Dana Avigail, *The Marker*, Cyber Supplement, October 2017; http://cybergirlz.org/wp-content/uploads/2017/10/their-way-to-cyber world.pdf; http://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/; www.csmonitor.com/World/Middle-East/2013/0609/Israel-accelerates-cybersecurity-know-how-as-early-as-10th-grade; Lior Tabansky and Isaac Ben-Israel 2015. 1, 27; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016; http://www.magshimim.cyber.org.il/; interview, Sagy Bar.
57. Interview, Sagy Bar; https://www.mamriot.cyber.org.il/; Government of Israel, Prime Minister's Office, National Cyber Directorate 2020.
58. Interview, Sagy Bar; Niv Ellis, Jerusalem Post, October 28, 2015. http://www.jpost.com/Business-and-Innovation/Health-and-Science/Multinationals-invest-in-teaching-Israeli-kids-to-code-430250; http://www.iati.co.il/news-item/1856/2016-national-coding-olympics-underway.
59. http://cyberknight.co.il/.

60. http://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/ ;https://www.chaire-cyber.fr/IMG/pdf/tr_article_3_21_-_chaire_cyberdefenseeng.pdf.
61. Interview, Tom Ahi Dror.
62. Interview, Sagy Bar.
63. https://he.wikipedia.org/wiki/%D7%9E%D7%92%D7%A9%D7%99%D7%9E%D7%99%D7%9D_-_%D7%AA%D7%95%D7%9B%D7%A0%D7%99%D7%AA_%D7%94%D7%A1%D7%99%D7%99%D7%91%D7%A8_%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99%D7%AA; http://www.rashi.org.il/—c1pcq; https://www.netonomy.com/blog/2018/01/22/interview-professor-isaac-ben-israel/; Isaac Ben-Israel, Meeting at the Belfer Center, Kennedy School of Government, September 14, 2017.
64. Sivan Klingweil, *The Marker*, January 23, 2020; https://she-codes.org/about/.
65. Shoshana Solomon, *Times of Israel*, August 28, 2019; Corinne Degani, *The Marker*, August 8, 2021.
66. Amitai Ziv, *Times of Israel*, September 12, 2019; Jack Hennessey, *Jerusalem Post*, January 27, 2022.
67. Interview, Tom Ahi Dror
68. Interviews with senior official #1, Tom Ahi Dror and senior officials #2 and 14; IISS 2021.
69. Yonah Jeremy Bob, *Jerusalem Post*, June 29, 2022 Amos Harel, *Haaretz*, September 25, 2022.
70. Interview, senior official #1; Frei 2020.
71. Amos Harel, *Haaretz*, September 25, 2022.
72. Interview, Tom Ahi Dror.
73. https://www.mako.co.il/news-military/2021_q3/Article-b861796623d7b71026.htm?utm_source=AndroidNews12&utm_medium=Share; Interview, senior official 2.
74. Dakota Cary, *Defense One*, July 23, 2021.
75. Inbal Orpaz, *Haaretz*, April 18, 2014; Christa Case Bryant, *Christian Science Monitor,* June 9, 2013, June 9, 2013; Amos Harel, *Haaretz,* November 14, 2013; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
76. Amos Harel, *Haaretz*, October 4, 2017.
77. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
78. Senor and Singer 2009.70–72; Baram and Ben-Israel, The Academic Reserve: Israel's Fast Track to High-Tech Success 2018; https://bit.ly/3LrOgBm.
79. Or Kashti, *Haaretz*, January 16, 2022.
80. Sophie Shulman, *Calcalist*, January 8, 2021.
81. Baram and Ben-Israel, The Academic Reserve: Israel's Fast Track to High-Tech Success 2018.
82. Christa Case Bryant, *Christian Science Monitor*, June 9, 2013; Cohen et al. 2015.5.
83. *Israel Defense*, May 1, 2017; Tal Inbar, *Israel Defense*, November 8, 2013; https://i-hls.com/archives/87804; Shmuel Even, David Siman-Tov and Gabi Siboni, *INSS Insight* September 21, 2016; Michal Danieli, *Mako*, April 10, 2011; http://tiny.cc/rp1y6y; Technological Courses http://tiny.cc/br0y6y; Yaakov Katz, *Jerusalem Post*, April 18, 2012; Ruti Levi, *The Marker*, January 14, 2019; Yoav Zitun, *Ynet* (English), July 24, 2015; David A. Fulghum, *Aviation Week & Space Technology*, August 2, 2010; Yaakov Lappin, *Jerusalem Post*, March 27, 2016; Yoav Stoler and Or Hirshaoga, *Calcalist*, March 29, 2018; http://tiny.cc/bkfz6y; https://www.idf.il/en/minisites/technology-and-innovation/educating-the-future-cyberwarfare-and-the-next-generation/; http://tiny.cc/dc6y6y;https://www.vredesactie.be/sites/default/files/BARCOisrael.pdf; https://www.jpost.com/Israel-News/Secretive-Talpiot-program-helps-IDF-soldiers-stay-ahead-of-the-curve-449279.
84. Inbal Orpaz, *Haaretz,* May 19, 2015.
85. http://www.*Haaretz*.com/israel-news/second-group-of-cyberdefenders-graduate-from-idf.premium-1.492778; http://zahal.com/2015/09/idfs-cyberdefenders-complete-training-course/.
86. Israel Ministry of Foreign Affairs, "Deputy FM Elkin: Israel's Cyber Security"; Yaakov Katz, *Jerusalem Post*, June 5, 2012.
87. https://www.idfblog.com/2017/01/02/model-city-trains-coders-stop-hacks/; https://www.ynetnews.com/articles/0,7340,L-4683636,00.html.
88. Amitai Ziv, *Haaretz* Weekend Magazine in English, May 30, 2019.
89. Amitai Ziv, *Haaretz* Weekend Magazine in English, May 30, 2019.

90. Amos Harel, *Haaretz*, September 25, 2022.
91. Sophie Shulman, *Calcalist*, January 8, 2021.
92. https://www.timesofisrael.com/idf-teaches-combat-soldiers-cyber-skills-as-springboard-to-civilian-life/.
93. Yossi Yehoshua, *YNet*, February 15, 2022.
94. Amir Mizroch, *Forbes*, May 28, 2018.
95. Shoshana Solomon, *Times of Israel*, July 22, 2019.
96. Senor and Singer 2009.67, 74; Swed and Butler 2013; Omer Keilaf, *Forbes*, July 3, 2020.
97. Amitai Ziv, *The Marker*, October 1, 2017.
98. Kahane 2012.942.
99. Tabansky and Ben-Israel 2015.18, 23; Baram and Ben-Israel 2018; Senor and Singer 2009.18, 51, 54; Kahane 2012.939, 943–945.
100. Senor and Singer 2009.70.
101. Kahane 2012.942; Omer Keilaf, *Forbes*, July 3, 2020.
102. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016; Adamsky 2017.122–123; Kahane 2012.943; Vijeta Uniyal, *Legal Insurrection*, June 23, 2016.
103. Freilich 2012.33–34, 44, 71; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
104. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
105. Arieli 2019.chapter 5.
106. Judy Rudoren and Isabel Kershner, *New York Times*, June 18, 2013; Adamsky 2017.110, 123.
107. Adamsky 2010.110.
108. Omer Keilaf, *Forbes*, July 3, 2020.
109. Tabansky and Ben-Israel 2015.20; Adamsky 2010.111, 117–118.
110. Senor and Singer 2009.50.
111. Senor and Singer 2009.74, 98; Tabansky and Ben-Israel 2015.20.
112. Peri 2006.69.
113. John Reed, *Financial Times*, July 10, 2015.
114. Sophie Shulman, *Calcalist*, January 8, 2021.
115. Sophie Shulman, *Calcalist*, January 8, 2021.
116. Sophie Shulman, *Calcalist*, January 8, 2021.
117. Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020.
118. http://www.*Haaretz*.com/israel-news/second-group-of-cyberdefenders-graduate-from-idf.premium-1.492778; Yaakov Katz, *Jerusalem Post*, May 31, 2012.
119. Sophie Shulman, *Calcalist*, January 8, 2021.
120. Sophie Shulman, *Calcalist*, January 8, 2021.
121. Senor and Singer 2009.54.
122. Taylor 2016.142, 146, 158–160.
123. Taylor 2016.159, 166.
124. Kahane 2012.941.
125. Taylor 2016.142, 161–164.
126. Senor and Singer 2009.232.
127. Swed and Butler 2013; Tabansky and Ben-Israel 2015.20.
128. Even and Siman-Tov 2012.22; Institute for National Security Studies and the Cyber Security Forum Initiative, 2014a; Swed and Butler 2013.
129. Swed and Butler 2013.
130. John Reed, *Financial Times*, July 10, 2015; Tabansky and Ben-Israel 2015.20; https://81amit.org.il/about/; https://www.9900.org.il/about.
131. Sophie Shulman, *Calcalist*, January 8, 2021.
132. http://www.ynetnews.com/articles/0,7340,L-4824677,00.html.
133. NoCamels Team, February 20, 2020.
134. Government of Israel, Prime Minister's Office, National Cyber Directorate 2020.
135. https://shoresh.institute/research-paper-eng-Ben-David-Kimhi-EducOverview.pdf.
136. Uri Berkowitz, *Globes*, November 4, 2020; Dana Yarkatzi, *Kan*, June 16, 2021; Government of Israel, Israel Innovation Authority 2021. 24.
137. Editorial, *Jerusalem Post*, October 16, 2014.

138. OECD 2015.178–179, 220; www.cbs.gov.il/reader/newhodaot/hodaa_template.html?hodaa=201606221; Omri Efraim, *Ynet*, December 29, 2015.
139. Israel Central Bureau of Statistics, media announcement, July 19, 2015.
140. This paragraph and the next are taken from Freilich 2018.148–149.
141. Shoshana Solomon, *Times of Israel*, December 16, 2018.
142. Nehemia Strassler, *Haaretz*, August 4, 2017; Stewart Winer, *Times of Israel*, January 16, 2017; Adir Yanko, *Ynet*, October 4, 2018; Meirav Arlozorov, *The Marker*, February 10, 2022.
143. http://www.readitnow.co.il/news, p. 293; Richet 2015; Ellen Nakashima and Ruth Eglash, *Washington Post*, May 14, 2016; Arad Atzmon Shmayer and Amitai Ziv, *The Marker*, July 11, 2019; Sammy Peretz, *The Marker,* April 22, 2018; Viva Sarah Press, *Israel21c.org*, August 3, 2015; Yossi Yehoshua, *Ynet*, November 29, 2021.
144. Government of Israel, Israel Innovation Authority 2021; https://i-hls.com/he/archives/82615; Amitai Ziv, *The Marker*, June 23, 2019, and January 22, 2020; Dana Yarkatzi, *Kan*, June 16, 2021.
145. Ruti Levy, *The Marker*, April 7, 2022.
146. Uri Berkowitz, *Globes*, November 19, 2019; *The Marker*, January 1, 2020, p. 21; https://swisscognitive.ch/2020/06/26/prof_isaac_ben_israel_cognitivenations_israel/.
147. Sagy Cohen, *The Marker*, December 22, 2020.
148. Amitai Ziv, *The Marker*, December 1, 2019; David Kramer, *Physics Today*, December 1, 2021; Sagy Cohen, *The Marker*, February 15, 2022.
149. https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/; https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate; https://www.theguardian.com/technology/2020/mar/10/questions-over-israels-role-in-whatsapp-lawsuit-against-spyware-firm-nso-group; https://www.Haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027; https://www.timesofisrael.com/report-israeli-spyware-helping-dictatorships-track-dissidents-minorities/; https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/.
150. https://www.timesofisrael.com/report-israeli-spyware-helping-dictatorships-track-dissidents-minorities/; https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.
151. Adamsky 2017.115; Siboni and Sivan-Sevilla 2017.94; Isaac Ben-Israel, Meeting at Belfer Center, September 14, 2017; https://www.theguardian.com/technology/2020/mar/10/questions-over-israels-role-in-whatsapp-lawsuit-against-spyware-firm-nso-group.
152. https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?module=inline; https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.
153. Interview, official #19.
154. Kurzak in Cornish 2021.486–492; For more specific details on the Wassenaar Agreement, see: https://www.wassenaar.org/; https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ; https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach.
155. https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/; https://www.telegraph.co.uk/technology/2019/05/14/whatsapp-flaw-allowed-israeli-hackers-snoop-phones/; https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate; https://www.theguardian.com/technology/2020/mar/10/questions-over-israels-role-in-whatsapp-lawsuit-against-spyware-firm-nso-group; https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?module=inline.
156. Dana Priest, Craig Timberg, and Souad Mekhennet, *Washington Post*, July 18, 2021; Craig Timberg, Michael Birnbaum, Drew Harwell, and Dan Sabbagh, *Washington Post*, July 20, 2121; Elizabeth Dwoskin and Shira Rubin, *Washington Post*, July 21, 2021; Craig Timberg and Drew Harwell, *Washington Post*, July 18, 2021; Shane Harris and Souad Mekhennet,

Washington Post, July 20, 2021; Ronen Bergman and Patrick Kingsley, *New York Times*, July 18, 2021; Phineas Rueckert, *Haaretz*, July 18, 2021; Amitai Ziv, *Haaretz*, July 20, 2021; Omer Kabir and Hagar Ravet, *Calcalist*, July 20, 2021; Katie Benner, David Sanger, and Julian Barnes, *New York Times*, December 3, 2021.

157. Shane Harris and Souad Mekhennet, *Washington Post*, July 20, 2021; Nina Fox, *Ynet*, July 21, 2021; Ronen Bergman and Mark Mazzetti, *New York Times*, July 17, 2021, and January 28, 2022; Amitai Ziv, *Haaretz*, July 20, 2021; Amos Harel, *Haaretz*, July 20, 2021.
158. https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private; https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html; https://www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html; https://www.israeldefense.co.il/en/node/52969; https://www.israeldefense.co.il/en/node/52969; https://www.reuters.com/technology/us-blacklists-four-companies-israel-russia-singapore-citing-spyware-2021-11-03/; Eric Martin, *Bloomberg Government*, November 3, 2021
159. Ronen Bergman and Mark Mazetti, *New York Times*, January 28, 2022; Ellen Nakashima, *Washington Post*, February 2, 2022.
160. https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/; https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate; https://www.theguardian.com/technology/2020/mar/10/questions-over-israels-role-in-whatsapp-lawsuit-against-spyware-firm-nso-group; https://www.timesofisrael.com/report-israeli-spyware-helping-dictatorships-track-dissidents-minorities/; https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.
161. Patrick Kingsley and Ronan Bergman, *New York Times*, February 7, 2022; *Haaretz*, February 8, 2022; Tomer Ganon, *Calcalist*, January 18, 2022; Chen Maanit, *Haaretz*, February 16, 2022.
162. *The Marker*, August 22, 2022.
163. https://www.cpomagazine.com/cyber-security/concerns-mount-as-israel-eases-rules-on-cyber-weapons-for-cyber-espionage/.
164. https://www.cpomagazine.com/cyber-security/concerns-mount-as-israel-eases-rules-on-cyber-weapons-for-cyber-espionage/.
165. Yoav Zitun, *Ynet*, December 6, 2021; Udi Etzion, *Calcalist*, December 16, 2021; Assaf Gilead, *Globes*, December 6, 2021; Meir Orbach, *Calcalist*, November 25, 2021; Amitai Ziv, *The Marker*, December 31, 2019; https://www.Haaretz.com/israel-news/.premium-for-intel-firms-changes-to-arms-treaty-could-make-hacking-phones-much-harder-1.8589323; https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.
166. https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach.
167. Schaake 2020.28; Morgan Meaker, *Wired*, August 15, 2022; https://www.axios.com/china-us-technology-surveillance-state-5672b822-fdde-45f9-ac77-e7b5574e9351.html;https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/; https://www.reuters.com/article/us-usa-spying-raven-specialreport/special-report-inside-the-uaes-secret-hacking-team-of-u-s-mercenaries-idUSKCN1PO19O; https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html; https://www.trtworld.com/magazine/the-uae-s-covert-web-of-spies-hackers-and-mercenary-death-squads-23805.

Chapter 9

1. INCD Annual Report 2020.
2. Amitai Ziv, *The Marker*, July 15, 2019, and December 31, 2020; Adamsky 2017.124; https://www.gov.il/he/departments/news/150720india.

3. Mueller et al. 2013; Cooper 2012a; Sofaer et al. 2010; Zittrain 2008.
4. Garcia 2015; Valeriano and Maness 2015.191, 198; Zittrain 2008.70; Sofaer et al. 2010.180.
5. http://www.thetower.org/3545oc-u-s-israel-sign-cybersecurity-intelligence-sharing-agreement/; http://www.worldbank.org/en/news/feature/2016/06/22/israel-shares-cybersecurity-expertise-with-world-bank-client-countries.
6. International Institute for Strategic Studies 2021.
7. Shoshana Solomon, *Times of Israel*, July 21, 2021; *Israel Defense*, July 22, 2021.
8. http://www.globes.co.il/en/article-us-congress-approves-israel-cyber-cooperation-1001163968.
9. http://mfa.gov.il/MFA/PressRoom/2016/Pages/Israel-and-the-US-sign-operative-cyber-defense-cooperation-agreement-21-June-2016.aspx; http://www.jpost.com/Israel-News/Politics-And-Diplomacy/US-Deputy-of-Homeland-Security-US-Israel-to-sign-automated-cyber-information-sharing-agreement-457261; http://www.thetower.org/3545oc-u-s-israel-sign-cybersecurity-intelligence-sharing-agreement/; http://legalinsurrection.com/2016/06/us-israel-sign-cyber-defense-agreement/; http://www.cyberwar.news/2016-07-01-u-s-israel-sign-beefed-up-cyber-defense-cooperation-agreement.html; https://www.csmonitor.com/World/Passcode/2017/0315/Event-Exploring-the-US-Israeli-relationship-in-cyberspace.
10. https://www.defense.gov/News/Article/Article/693128/carter-israeli-counterpart-agree-to-increased-cyber-cooperation/.
11. Mandi Kogosowski, *Israel Defense*, April 21, 2021.
12. https://www.congress.gov/bill/114th-congress/house-bill/5843; https://www.congress.gov/bill/114th-congress/house-bill/5843;%20; http://www.globes.co.il/en/article-us-congress-approves-israel-cyber-cooperation-1001163968.
13. http://www.timesofisrael.com/nsa-chief-makes-secret-israel-trip-to-talk-iran-hezbollah-cyber-warfare/.
14. Yaakov Lapin, *JNS*, December 1, 2021; Shoshana Solomon, *Times of Israel*, July 9, 2019; INCD Annual Report 2020.
15. Shoshana Solomon, *Times of Israel*, July 2, 2017; Amanda Ngo, *NoCamels*, June 28, 2017.
16. Nicole Perloth and David Sanger, *New York Times*, May 15, 2018.
17. INCD Annual Report 2020.
18. https://therecord.media/inglis-sworn-in-as-first-national-cyber-czar/.
19. *Reuters*, November 14, 2021; Rina Bassist, *al Monitor*, August 25, 2022.
20. Lahav Harkov, *Jerusalem Post*, September 27, 2022; Jacob Magid, *Times of Israel*, September 28, 2022; https://www.haaretz.com/israel-news/2022-07-14/ty-article/full-text-joint-u-s-israel-jerusalem-declaration-signed-by-biden-and-lapid/00000181-fbd0-d4e2-a193-fffec7da0000.
21. Shortly after the agreement was signed, Boeing and the INCD concluded an aircraft industry cyber security deal, providing for an exchange of intelligence, means of identifying and mitigating potential threats, and joint work on a variety of defensive solutions.
22. Yonah Jeremy Bob, *Jerusalem Post*, July 3, 2022; Jerusalem Post staff, July 27, 2022; Rina Bassist, *al Monitor*, August 25, 2022; Carrie Keller-Lynn, *Times of Israel*, February 2, 2022.
23. Yonah Jeremy Bob, *Jerusalem Post*, August 9, 2022; Rina Bassist, *al Monitor*, August 25, 2022.
24. Yaakov Lappin, *JNS*, January 23, 2020.
25. Udi Shaham, *Jerusalem Post*, February 1, 2021.
26. Yonah Jeremy Bob, *Jerusalem Post*, June 29, 2022.
27. Consultations held by authors with interested parties.
28. https://mfa.gov.il/MFA/ForeignPolicy/MFADocuments/Yearbook12/Pages/83%20Israel-US%20Memorandum%20on%20Strategic%20Cooperation-.aspx.
29. Interviews, senior officials #1, #2, #7 and Ronen Korman.
30. Eisenstadt and Pollock 2012.36; https://i-hls.com/archives/59568.
31. Gil Press, *Forbes*, April 12, 2018; https://www.haaretz.com/israel-news/business/study-israeli-founded-firms-bring-9-3-billion-to-massachusetts-1.5393343.
32. http://www.usisraelbusiness.com/files/2015/03/US-Israel-Cyber-Task-Force.pdf?ce474b.
33. "BGU, UA and UNAM Sign Agreement." *Ben Gurion University of the Negev*, September 19, 2017; https://tech.cornell.edu/news/cornell-tech-campus-opens-on-roosevelt-island-marking-transformational-mile/.

34. Simona Shemer, *NoCamels*, October 3, 2018; NoCamels Team February 4, 2020.
35. *Economist*, Israel's Ties with China Are Raising Security Concerns, October 11, 2018; Greenert and Bird 2020.45.
36. Greenert and Bird 2020; Amos Harel, *Haaretz*, January 16, 2019, July 5, 2019; Scott Moore, *Wired*, December 19, 2018.
37. *Economist,* Israel's Ties with China Are Raising Security Concerns, October 11, 2018.
38. Amos Harel, *Haaretz*, January 7, 2019.
39. Herb Canaan, *Jerusalem Post*, October 30, 2019; Greenert and Bird 2020.41; Yonah Jeremy Bob, *Jerusalem Post*, April 17, 202; Lahav Harkov, *Jerusalem Post*, August 15, 2020; Segev 2020; https://dk.usembassy.gov/the-clean-network-safeguards-americas-assets/.
40. Assaf Orion, *Beyond Chastity Belt and Road: US-Israeli Relations in the Age of Great Power Competition*, Policy Analysis, Washington Institute, February 6, 2022.
41. Matania and Rappaport, Cybermania, 2021.737–738.
42. https://www.gov.uk/government/news/uk-and-israel-sign-memorandum-of-understanding-mou-on-digital-government.
43. Dan Sabbagh, *Guardian,* November 28, 2021; Tzvi Joffre, *Jerusalem Post*, November 29, 2021; Emilio Casalicchio, *Politico*, November 29, 2021; https://www.infosecurity-magazine.com/news/uk-israel-cooperation-cybersecurity/.
44. https://www.thejc.com/news/uk-news/revealed-gchq-s-israel-uk-partnership-1.431416; Barak Ravid and Oded Yaron, *Haaretz*, April 26, 2017; Matania and Rappaport, Cybermania, 2021.773–777.
45. Press Release, Israeli and UK Academics to Combat Global Cyber Security Threats, March 24, 2015, The UK Cabinet Office, The Rt Hon Lord Maude of Horsham and Government Digital Service; Ami Rojkes Dombe, *Israel Defense*, September 17, 2015.
46. Press Release, Israeli and UK Academics to Combat Global Cyber Security Threats, March 24, 2015, The UK Cabinet Office, The Rt Hon Lord Maude of Horsham and Government Digital Service; https://www.gov.uk/government/topical-events/d5-london-2014-leading-digital-governments; https://www.gov.uk/government/news/uk-hosts-d5-the-first-digital-leaders-summit; https://en.wikipedia.org/wiki/Digital_Nations; https://www.leadingdigitalgovs.org/.
47. https://www.israel21c.org/uk-israel-tech-hub-celebrates-175-partnerships-54-deals/.
48. http://www.hindustantimes.com/india-news/india-israel-set-to-enlarge-web-of-ties/story-zE5EZAxjGDTvRXmHMXwWEO.html; https://besacenter.org/wp-content/uploads/2017/07/547-PM-Modis-Visit-to-Israel-Gupta-final.pdf;. https://www.timesofisrael.com/india-israel-set-to-team-up-on-cyber-defense/; https://www.businesstoday.in/current/economy-politics/full-text-of-india-israel-joint-statement-on-trade-defence-security/story/268089.html; https://thewire.in/diplomacy/india-israel-cyber-security-partnership; https://tech.economictimes.indiatimes.com/news/corporate/israel-looks-to-collaborate-with-india-other-countries-to-build-cyber-shields/64802121; Dipanjan Roy Chaudhury, *Economic Times*, January 16, 2018.
49. https://itrade.gov.il/india/2020/01/30/cyber-edge-israeli-cyber-delegation-visit-to-india-16-17-december-2019/; https://www.jpost.com/Israel-News/Israeli-cybersecurity-envoy-trains-with-Indian-counterparts-611730.
50. https://www.cybervie.com/blog/cooperation-in-cybersecurity/; *The Hindu*, July 16, 2020.
51. http://hamodia.com/2017/05/11/israel-japan-increase-cyber-economic-cooperation/.
52. Sharon Udasin, *Jerusalem Post*, May 3, 2017.
53. Shoshana Solomon, *Times of Israel*, December 2, 2015.
54. Eyal Ben-Ari, Japan-Israel Collaboration, JISS, September 12, 2022.
55. http://www.jewishpress.com/news/politics/watch-netanyahu-tell-japans-foreign-minister-we-both-live-in-challenging-regions/2017/12/25/.
56. Clint Richards, *The Diplomat*, May 13, 2014.
57. Matania and Rappaport, Cybermania, 2021.675.
58. Ricky Ben David, *Times of Israel*, November 17, 2021.
59. Eyal Ben-Ari, Japan-Israel Collaboration, JISS, September 12, 2022.
60. *Defence Connect*, October 31, 2017.

61. "Australia Israel Joint Statement," *Prime Minister's Office of Israel*, February 23, 2017; http://www.australiandefence.com.au/defence/cyber-space/pm-signs-cyber-security-mou-with-israel; https://ministers.pmc.gov.au/tehan/2017/joint-outcomes-australia-israel-leaders-roundtable-cyber-security; https://www.defenceconnect.com.au/key-enablers/1466-australia-and-israel-sign-defence-industry-agreement.
62. http://www.israelscienceinfo.com/en/finance/israel-australie-accord-sans-precedent-de-rd-en-cyber-securite-avec-la-commonwealth-bank/.
63. http://mfa.gov.il/MFA/InnovativeIsrael/Economy/Pages/Technological-R-and-D-cooperation-agreement-signed-with-New-South-Wales-7-April-2016.aspx.
64. "The Cyberwarfare Market 2012–2022," *PR Newswire* (New York), December 19, 2011; Viva Sarah Press, *Israel21c*, July 9, 2015; *Progressive Digital Media Technology News*, September 14, 2016; Eliran Rubin, *Haaretz*, October 30, 2017; Viva Sarah Press, *Israel21c*, June 15, 2015; http://tlabs.bgu.ac.il/index.php/the-news/137-deutsche-telekom-innovation-laboratories-at-bgu-dedicates-expanded-offices.
65. https://www.reuters.com/article/us-germany-israel-cyber/german-israeli-companies-to-cooperate-on-cybersecurity-idUSKBN17E0WL; http://www.iati.co.il/news-item/2309/iati-signs-mou-cyber-security-council-germany-cscg.
66. http://www.international.gc.ca/name-anmo/canada_israel_MOU-prot_ent_canada_israel.aspx?lang=eng.
67. Sharon Udasin, *Jerusalem Post*, May 23, 2017; *Reuters*, October 4, 2017.
68. https://www.calcalistech.com/ctech/articles/0,7340,L-3874096,00.html; https://www.cyberscoop.com/israel-uae-cybersecurity-deal-tech-firms/; https://www.mei.edu/publications/how-tech-cementing-uae-israel-alliance; https://www.ft.com/content/67c28071-2e9a-4d06-a264-b543f5e4de9e.
69. Dion Nissenbaum and Dov Lieber, *Wall Street Journal*, July 12, 2022.
70. https://www.lexology.com/library/detail.aspx?g=fe239ade-24a8-461d-ba6f-bc34162a7af2; https://www.calcalistech.com/ctech/articles/0,7340,L-3903464,00.html; https://www.mei.edu/publications/how-tech-cementing-uae-israel-alliance; https://www.jns.org/dubai-conference-highlights-online-security-issues-cooperation-with-israel-on-cyber-defense/.
71. https://www.cyberscoop.com/israel-uae-cybersecurity-deal-tech-firms/; https://www.mei.edu/publications/how-tech-cementing-uae-israel-alliance; https://www.timesofisrael.com/liveblog_entry/uae-cyber-official-says-israel-emirates-cooperating-on-threats/; https://www.egic.info/israel-gulf-cyber-cooperation; https://www.reuters.com/article/us-israel-gulf-emirates-cyber-idUKKCN26F2UK; https://www.jpost.com/middle-east/uae-cyber-head-israeli-intel-sharing-helps-deter-hacking-attempts-643457; https://www.israeldefense.co.il/en/node/49182; https://www.ft.com/content/67c28071-2e9a-4d06-a264-b543f5e4de9e; https://insidearabia.com/uae-israel-cyber-spying-aids-emirati-influence-and-repression/; https://moderndiplomacy.eu/2020/12/23/israeli-gulf-cyber-cooperation/; https://www.israelhayom.com/2021/06/25/israels-rafael-defense-firm-unveils-new-consortium-to-provide-cyber-security-in-dubai/.
72. https://www.egic.info/israel-gulf-cyber-cooperation.
73. Tovah Lazaroff, *Jerusalem Post*, July 17, 2021.
74. Hagai Amit, *Haaretz* (English), August 12, 2021.
75. Dion Nissenbaum and Dov Lieber, *Wall Street Journal*, July 12, 2022.
76. Yonah Jeremy Bob, *Jerusalem Post Magazine*, December 10, 2020; https://www.defensenews.com/global/2016/04/19/israel-singapore-pledge-expanded-cyber-cooperation/; https://version-2.com.sg/2020/10/version-2-singapore-singapore-is-strengthening-its-cyber-security-capabilities-by-collaborating-with-israels-tel-aviv-university/; https://www.straitstimes.com/tech/spore-cyber-security-capabilities-to-be-enhanced;https://ice71.sg/events/event/cyber-startup-fiesta-showcasing-israel/; https://www.cancham.org.sg/events/collaboration-opportunities-with-israeli-cyber-security-innovation; https://www.sgtech.org.sg/SGTECH/Web/SGTech_News_2020/Jul20/Collaboration_Opportunities_with_Israeli_Cyber_Innovations.aspx; https://www.sginnovate.com/events/national-cybersecurity-partnership-singapore-and-israel; https://cyberweek.tau.ac.il/2019/Events/Singapore-%7Cfwsa%7C-Israel-Roundtable; https://www.israelhayom.com/2018/10/17/singapore-investment-giant-buys-israeli-%E2%80%8Ecybersecur

ity-startup-for-250-million-%E2%80%8E/; https://www.cnbc.com/2018/10/16/singapore-firm-temasek-to-acquire-israeli-cybersecurity-firmsygnia-.html; https://www.jpost.com/cybertech/cyber-consulting-co-sygnia-opens-apac-headquarters-in-singapore-630162; https://nocamels.com/2015/03/infocomm-to-invest-up-to-200m-in-israeli-startups/; https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/?sh=3134de20420a; https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/; https://www.asianscientist.com/2017/02/tech/ntu-bgu-bioinspired-agile-cybersecurity-assurance-framework/; http://blavatnikfoundation.org/the-blavatnik-icrc-brings-together-israel-uae-and-singapore-for-cyber-pandemic-webinar/; link.gale.com/apps/doc/A491282777/STND?u = mlin_n_merrcol&sid = STND&xid = fef161fd, accessed February 22, 2021; "Israeli Cybersecurity Think Tank, Team8, Partners with Temasek, Singtel, SGX and CIO Academy to Bring Its Global Thought Leadership Event Series, Rethink Cyber, for the First Time to Singapore," *PR Newswire Europe*, May 8, 2017; *Gale OneFile: News*; "Votiro Signs Distribution Agreement with Netpoleon Solutions to Provide Companies in Singapore with Cyber Security Solutions for Zero-Day and Undisclosed Exploits," *PRN Asia*, December 13, 2016; *GaleOneFile: News*, link.gale.com/apps/doc/A473761604/STND?u = mlin_n_merrcol&sid = ebsco&xid = 5d7fba04, accessed 29 July 2021; "Sygnia, Elite Cyber Consulting and Incident Response Company Launched by Team8, To Be Acquired by Temasek," *PR Newswire*, October 16, 2018. *Gale Academic OneFile*, link.gale.com/apps/doc/A558366770/AONE?u = mlin_n_merrcol&sid = AONE&xid = 0814f8a6, accessed February 22, 2021; "Sygnia, an Elite Cyber Consulting and Incident Response Company, Announces the Opening of Its APAC Headquarters in Singapore," *PRN Asia*, May 27, 2020; *Gale OneFile: News*, link.gale.com/apps/doc/A625018027/STND?u = mlin_n_merrcol&sid = ebsco&xid = a6bd5de3, accessed July 29, 2021; "ICE and GamaSec Partner for Asia Cyber Insurance Venture," *Legal Monitor Worldwide*, March 11, 2021; *Gale General OneFile*, link.gale.com/apps/doc/A654538271/ITOF?u = mlin_n_merrcol&sid = ebsco&xid = e1580af6, accessed July 29, 2021; "Singapore Gears up to Boost Investment in Israel," *Singapore Government News*, March 2, 2015. *Gale OneFile: News*, link.gale.com/apps/doc/A403677481/STND?u = mlin_n_merrcol&sid = STND&xid = 213030ad, accessed February 22, 2021; "RSA Eyes Singapore Talent to Accelerate Cyber Security Skills Training," *PR Newswire*, 5 June 2013; *Gale OneFile: News*, link.gale.com/apps/doc/A332502554/STND?u = mlin_n_merrcol&sid = ebsco&xid = 85172604; accessed July 29, 2021; "Check Point Software Technologies Partners with Singapore Polytechnic to Strengthen Cyber Security Skills in Singapore." *ENP Newswire*, 31 May 2019; *Gale Academic OneFile Select*, link.gale.com/apps/doc/A587258752/EAIM?u = mlin_n_merrcol&sid = ebsco&xid = be4d6658, accessed July 29, 2021.

77. https://www.intelligenceonline.com/international-dealmaking/2019/04/03/singapore-turns-to-israeli-cyber-spies-again,108351899-art; https://www.haaretz.com/israel-news/business/.premium-tech-nation-1.5322591; https://www.defensenews.com/global/2016/04/19/israel-singapore-pledge-expanded-cyber-cooperation/; https://en.globes.co.il/en/article-iai-singapore-unit-awarded-cybersecurity-project-1001326330; https://www.defenseworld.net/news/26819/Israeli_ELTA_to_Partner_Singapore_DSTA_in_Cybercrimes_Detection#.YQK3FehJNPY; IAI Awarded Cybersecurity Project in Singapore, *Legal Monitor Worldwide*, April 27, 2020; *Gale GeneralOneFile*, link.gale.com/apps/doc/A622060727/ITOF?u = mlin_n_merrcol&sid = ITOF&xid = a40d6964, accessed February 22, 2021.
78. https://www.israeldefense.co.il/en/content/israel-and-italy-signed-declaration-cyber-collaboration.
79. https://embassies.gov.il/athens/NewsAndEvents/Pages/IsraelCyprusGreece5thTrilateralSummitDeclaration.aspx; https://besacenter.org/greece-defense-industry/.
80. Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020; https://portswigger.net/daily-swig/cross-border-collaboration-israel-and-romania-sign-cybersecurity-partnership.
81. Yonah Jeremy Bob, *Jerusalem Post*, December 10, 2020.
82. INCD Annual Report 2020.
83. INCD Annual Report 2020; Eli Horn, *Israel Defense*, November 14, 2020.

84. http://www.worldbank.org/en/news/feature/2016/06/22/israel-shares-cybersecurity-expertise-with-world-bank-client-countries.
85. Eytan Halon, *Jerusalem Post*, June 18, 2019; Francine Levy, *NoCamels*, June 17, 2019.
86. Amitai Ziv, *The Marker*, July 15, 2019; IISS 2021; INCD Annual Report 2020; https://www.israeldefense.co.il/en/node/50340.
87. *Times of Israel* Staff, December 9, 2021.
88. https://www.idf.il/en/minisites/technology-and-innovation/the-idf-hosted-its-first-international-digital-and-cyber-convention/; Yaakov Lappin, *JNS*, January 23, 2020.
89. Interview, senior official #20.
90. Government of the United States 2020.46.
91. Finnemore and Hollis 2016.436–437.
92. Finnemore and Hollis 2016.439, 442; Benoliel 2015.441, 480.
93. Benoliel 2015.435–436, 440.
94. Choucri 2012.168; Finnemore and Hollis 2016.437–438; https://en.wikipedia.org/wiki/Convention_on_Cybercrime#cite_note-4.
95. David Ignatius, *Washington Post*, October 24, 2017, and January 2, 2020; Laura Rosenberger 2020.
96. Hurwitz 2014.322–331; Tabansky 2020.73; Rosenberger 2020; Segev 2020; Jasper 2017.144–145, 148; IISS 2021; David Ignatius, *Washington Post*, July 20, 2021; Greenhouse and Barros 2020.
97. UN Report 2021.
98. Group of Governmental Experts, 2015; Jasper 2017.147–148; Buchanan 2017.134–136; Benoliel 2015.441; Even and Siman-Tov 2012.44.
99. Schmitt 2013; Eilstrup-Sangiovanni 2018; Jasper 2017.14, 91, 94.
100. https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis.
101. David Ignatius, *Washington Post*, March 30, 2021.
102. https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis.
103. Rosenberger 2020.
104. Cat Zakrzewski, *Washington Post*, November 13, 2018; Louise Matsakis, *Wired*, November 12, 2018; Joe Uchill, *Axios*, November 12, 2018.
105. Valeriano and Maness 2015.77; Blank 2013.426–427, 434–435.
106. Nye 2016–2017.61; Eichensher 2015.364, 373; Eilstrup-Sangiovanni 2017; Blank 2013.21–22, 415; Schmitt 2012.21–22; Schmitt 2013; Schmitt 2017.22, 36, 38; Blank 2013.415; https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; https://wnoww.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf p.744.
107. https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
108. Lin 2010.78.
109. Crosston 2013.123; Schmitt 2012.30; Tallinn Manual note 5, R. 39 cmt. 4; Schaake 2020.28.
110. Interview, senior official #18; Schaake 2020.28.
111. Tabansky 2012.73; Finnemore and Hollis 2016.437–438; Even and Siman-Tov 2012.44–45; Hurwitz 2014.329.
112. https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
113. O'Connell, 2015.519, 525; Schmitt 2013.
114. Schmitt 2012.20; Tallinn Manual, note 5, R. 11 cmts. 4,5.
115. Eilstrup-Sangiovanni 2017.
116. Jervis 1978.202; Brown and Friedman 2014.56; Nye 2016–2017.61.
117. Nye 2016–2017.60; Sofaer, Clark, and Diffie in National Research Council 2010.192–193
118. Brown and Friedman 2014.57; Crosston 2013.120–121.
119. Sofaer, Clark, and Diffie in National Research Council 2010.191.
120. Schöndorf 2020; Schmitt 2020.

121. Interview, senior official #23.
122. Matania and Rappaport, Cybermania, 2021.864–867.
123. Schmitt 2020, Part 1.
124. Matania and Rappaport, Cybermania, 2021.669.
125. Blank 2013; Schmitt 2012.20.
126. Joe Uchill, *The Hill*, September 13, 2016.
127. Finnemore and Hollis 2016.437–438; Even and Siman-To 2012.44–45; Nye 2010.18; Sofaer, Clark, and Diffie in National Research Council 2010.194.
128. Valeriano and Maness 2015.440.

Chapter 10

1. Yakov Katz, *Jerusalem Post*, May 31, 2012; Fulghum 2012.
2. IDF Strategy 2015.18; IDF Strategy 2018.18, 19, 21, 29.
3. Interviews, senior officials #3, #4, and #5 and Eviatar Matania.
4. *Maarachot*, May 2017.1.
5. Interview, senior official #6.
6. Interview, senior official #16.
7. Matania and Rappaport, *Cybermania*, 2021.222.
8. Interview, Yair Golan.
9. Interview, Eviatar Matania.
10. Freilich 2018.225–229.
11. Interview, senior official #1.
12. IDF Strategy 2018.18, 19, 21, 29; Cohen 2013.10–11; https://go.YNet.co.il/pic/news/16919.pdf pp.18–19, 30, 31.
13. http://www.YNet.co.il/articles/0,7340,L-4981390,00.html: http://www.nrg.co.il/online/1/ART2/883/971.html.
14. Amitai Ziv, *The Marker*, October 1, 2017.
15. Yonah Jeremy Bob, *Jerusalem Post*, June 24, 2015.
16. Israel National Cyber Directorate, June 26, 2019.
17. Interview, Eviatar Matania.
18. Yonah Jeremy Bob, *Jerusalem Post*, June 24, 2015, and April 28, 2016.
19. Yonah Jeremy Bob, *Jerusalem Post*, February 1, 2017.
20. Yonah Jeremy Bob, *Jerusalem Post*, June 18, 2018, and August 25, 2018.
21. Yoav Zitun, *YNet*, September 27, 2021.
22. Colonel A. et al., September 27, 2021.149, 157.
23. Interview, senior official #10.
24. Interview, senior officials #1 and #15.
25. Interview, senior officials #1, #2, and #12.
26. Interview, senior official #15.
27. Interview, senior officials #3 and #4.
28. Interview, senior officials #1, #5, and #6.
29. Nir Dvori, *N12*, December 10, 2020.
30. Interview, senior officials 1#, #3, and #4.
31. Interview, senior officials #3, #4, and #12.
32. Interview, senior official #7.
33. Interviews, senior officials #3, #4 and #5.
34. Amos Harel, *Haaretz*, November 7, 2019; Yaakov Lappin, *Jerusalem Post*, August 17, 2014, and September 18, 2015; Yoav Zitun, *YNet*, September 2, 2015; Nir Dvori, *Mako*, April 18, 2019; https://www.c4isrnet.com/battlefield-tech/2020/02/05/israel-finds-an-ai-system-to-help-fight-in-cities/.
35. Amitai Ziv, *The Marker*, September 22, 2020.
36. Yoav Zitun, *YNet*, February 9, 2021.
37. Amos Harel, *Haaretz*, November 7, 2019; Yaakov Lappin, *Jerusalem Post*, August 17, 2014, and September 18, 2015; Yoav Zitun, *Ynet*, September 2, 2015; Nir Dvori, *Mako*, April 18, 2019; https://www.c4isrnet.com/battlefield-tech/2020/02/05/israel-finds-an-ai-system-to-help-fight-in-cities/.

38. Itam Elmadon, *N12*, January 21, 202
39. Tabansky 2020.6.
40. IISS 2021.
41. Yoav Zitun, *YNet*, January 25, 2012.
42. Yaakov Lappin, *Jerusalem Post*, July 27, 2015.
43. Yoav Zitun, *YNet*, October 29, 2020.
44. Interviews, senior officials #3, #4, and #5.
45. Interviews, senior officials #7 and #12.
46. Interview, senior official #7.
47. Interview, senior official #11.
48. Amos Harel, *Haaretz*, August 20, 2018; TOI Staff, *Times of Israel*, January 29, 2016.
49. Itam Elmadon, *N12*, January 21, 2021.
50. Yoav Zitun, *YNet* (English), May 8, 2017.
51. Amos Harel, *Haaretz*, September 21, 2022.
52. Shoshana Solomon, *Times of Israel*, November 21, 2018; Itam Elmadon, *N12*, January 21, 2021.
53. Ronen Bergman, *Ynet* (English), December 12, 2012; Tova Dvorin, *Arutz Sheva*, April 25, 2014; Yaakov Lappin, *Jerusalem Post*, February 13, 2014.
54. Israel Wulman, *YNet* (English), June 24, 2016.
55. Yonah Jeremy Bob, *Jerusalem Post*, August 25, 2018.
56. Judah Ari Gross, *Times of Israel*, August 15, 2018; Yoav Zitun, *YNet*, January 11, 2017; http://bit.ly/2Z3Xn2N; http://www.YNetnews.com/articles/0,7340,L-4906289,00.html; https://www.Haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773; http://www.israeldefense.co.il/en/node/28217; https://en.globes.co.il/en/article-hamas-preparing-for-cyber-war-1001246720.
57. Judah Ari Gross, *Times of Israel*, August 15, 2018; Yoav Zitun, *YNet*, January 11, 2017; http://bit.ly/2Z3Xn2N; http://www.YNetnews.com/articles/0,7340,L-4906289,00.html; https://www.Haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773; http://www.israeldefense.co.il/en/node/28217; https://en.globes.co.il/en/article-hamas-preparing-for-cyber-war-1001246720.
58. Oded Yaron, *Haaretz*, November 28, 2018.
59. Amos Harel, *Haaretz*, September 21, 2022.
60. Cohen 2013.10–11.
61. See Freilich 2018.chapter 8 for a detailed analysis of Israel's nuclear policy and the Begin Doctrine, the salient points raised there are summarized in this section; Long in Lin and Zegart 2019.108.
62. Amos Harel, *Haaretz*, September 3, 2013, and October 18, 2013.
63. Jerusalem Post Staff, *Jerusalem Post*, August 7, 2015; www.haaretz.com/israel-news/israel-s-mossad-trained-assassins-of-iran-nuclear-scientists-report-says-1.411945; www.theguardian.com/world/julian-borger-global-security-blog/2012/jul/11/israel-iran-nuclear-assassinations; www.israeltoday.co.il/NewsItem/tabid/178/nid/23644/Default.aspx; www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.
64. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.
65. Government of the United Kingdom 2021.
66. Farrell and Glaser in Lin and Zegart 2019.52–53.
67. Katzir 2015.103, 111.
68. Amitai Ziv, *The Marker*, October 1, 2017.
69. Chachko 2020.8–9.
70. Frei 2020; Tal Shachaf, *YNet*, May 21, 2021; Judah Ari Gross, *Times of Israel*, May 14, 2007; Amitai Ziv, *The Marker*, October 1, 2017.
71. Raska 2015.4–5.
72. Raska 2015.4–5.
73. https://en.wikipedia.org/wiki/Unit_8200.
74. John Reed, *Financial Times*, July 10, 2015; Frei 2020.

75. Anna Ahronheim, *Jerusalem Post*, February 21, 2018.
76. Interview, senior officials #3 and #4.
77. Yoav Zitun, *YNet* (English), June 15, 2015; Barbara Opall-Rome, *Defense News*, June 18, 2015; Adamsky 2017.120.
78. Interview, senior official #4.
79. Interview, senior officials # 2 and #4.
80. Interview, senior officials #2, #7, and #15.
81. Interview, senior official #7.
82. Interview, senior officials #16 and #17.
83. Interview, senior officials #7 and #15.
84. Judah Ari Gross, *Times of Israel*, May 14, 2007; Amitai Ziv, *The Marker*, October 1, 2017.
85. Interview, senior official #17.
86. Interview, Gadi Eisenkot.
87. Ronen Bergman, *Ynet* (English), December 12, 2012; Tova Dvorin, *Arutz Sheva*, April 25, 2014; Yossi Melman, *Maariv*, August 12, 2017; Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
88. Yossi Melman, *Maariv*, August 12, 2017.
89. Matania and Rappaport, *Cybermania*, 2021.222, 225, 228–236.
90. Eichner, Itamar *YNet* (English), January 18, 2017; Yonah Jeremy Bob, *Jerusalem Post*, October 2, 2020.
91. Amir Rapaport, *Israel Defense*, September 5, 2014; Ben-David 2011.57; Yakov Katz, *Jerusalem Post*, May 31, 2012.
92. Gili Cohen, *Haaretz*, June 27, 2017; Yonah Jeremy Bob, *Jerusalem Post*, October 2, 2020.
93. Ellen Nakashim and William Booth, *Washington Post*, May 14, 2016.
94. Yonah Jeremy Bob, *Jerusalem Post*, October 2, 2020.
95. Itamar Eichner, *YNet* (English), January 18, 2017; Yonah Jeremy Bob, *Jerusalem Post*, October 2, 2020.
96. Yossi Melman; *Haaretz*, November 16, 2021; https://www.israeldefense.co.il/he/node/39083; Yakov Katz, *Jerusalem Post*, May 31, 2012; Yonah Jeremy Bob, *Jerusalem Post*, March 22, 2013; IISS 2021.
97. Itai Ilnai, *YNet*, January 14, 2022.
98. Yakov Katz, *Jerusalem Post*, May 31, 2012; Yonah Jeremy Bob, *Jerusalem Post*, March 22, 2013.
99. David Horovitz, *Times of Israel*, February 6, 2019.
100. Yonah Jeremy Bob, *Jerusalem Post*, June 20, 2016.
101. http://www.jpost.com/Israel-News/Is-Israel-equip-to-handle-demands-of-the-evolving-realm-of-cybercime-490897.
102. https://www.intelligence-research.org.il/editor/assets/collaborative-leadership.pdf.
103. Interview, senior official #13.
104. Interview, senior official #13.
105. Interview, Ronen Korman.
106. Interview, Eviatar Matania.
107. Interviews, Ronen Korman and senior official #13.
108. Interview, senior official #13.
109. Rid 2013.45.
110. Schmidt and Cohen 2014.106; Heckman et al. 2015.54–55, 60; Zetter 2014.
111. Heckman et al. 2015.54–55; Schmidt and Cohen 2014.106; Sanger 2018.7, 21; Rid 2013.43–45.
112. Zetter and Modderkolk 2019.
113. Sanger 2018.21.
114. Heckman et al. 2015.54–55; Schmidt and Cohen 2014.106; Sanger 2018.7, 21.
115. Segal 2017; Sanger 2018.29.
116. Ari Shavit, *Haaretz*, August 9, 2012; Freilich 2018.207, 249.
117. Sanger 2018.7; Valeriano and Maness 2015.151.
118. Sanger 2018.29.
119. Brantly 2018.60.
120. Freilich 2012.207.

121. Sanger 2018.27–29.
122. Freilich 2012.207.
123. Yakov Katz, *Jerusalem Post*, May 31, 2012; Sanger 2018.9; http://www.richardsilverstein.com/2012/10/23/idf-to-double-unit-8200-cyber war-manpower/; Rid 2013.96.
124. Ellen Nakashima and William Booth, *Washington Post*, May 14, 2016.
125. Anderson and Sadjadpour 2018.10; Segal 2017.4; Segal, A. *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Ages*. New York: Public Affairs (2017), p.4; https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks; https://resources.infosecinstitute.com/topic/duqu-2-0-the-most-sophisticated-malware-ever-seen/; https://www.spiegel.de/international/world/israel-thought-to-be-behind-new-malware-found-by-kaspersky-a-1037960.html; Valeriano and Maness 2015.151.
126. Segal 2017.149; Kim Zetter, *Wired*, May 28, 2012; Ellen Nakashima, Greg Miller, and Julie Tate, *Washington Post*, July 19, 2012; Schmidt and Cohen 2014.107.
127. Segal 2017.4, 149; Serif Bahtiyar, Mehmet Barıs Yaman, and Can Yılmaz Altınigne, *Computer Networks*, September 19, 2019.120; Rid 2013.94–95; Lemay et al. 2018.44–45; Kim Zetter, *WIRED*, May 28, 2012.
128. https://www.crysys.hu/publications/files/skywiper.pdf.
129. Kim Zetter, *Wired,* May 28, 2012; Serif Bahtiyar, Mehmet Barıs Yaman, Can Yılmaz Altınigne, *Computer Networks*, September 19, 2019.120; Lemay et al. 2018.44–45.
130. Kim Zetter, *Wired,* May 28, 2012.
131. Segal 2017.149.
132. Anderson and Sadjadpour 2018.10; Segal 2017.149.
133. Segal 2017.149; Kim Zetter, *Wired*, May 28, 2012.
134. Anderson and Sadjadpour 2018.10; Segal 2017.149.
135. Segal 2017.4, 149; https://www.bbc.com/news/technology-18365844.
136. Schmidt and Cohen 2014.107.
137. https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.
138. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf; Samuel Gibbs, *The Guardian*, June 11, 2015.
139. Rid 2013.94.
140. Lemay et al. 2018.44–45.
141. https://securelist.com/duqu-faq-33/32463/; https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet; Lemay et al. 2018.44–45; Rid 2013.94.
142. https://securelist.com/duqu-faq-33/32463/; https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.
143. https://securelist.com/duqu-faq-33/32463/.
144. https://www.symantec.com/security-center/writeup/2011-101814-1119-99.
145. https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet; https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf; https://securelist.com/duqu-faq-33/32463/.
146. https://securelist.com/duqu-faq-33/32463/; https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.
147. Samuel Gibbs, *The Guardian*, June 11, 2015.
148. https://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/; Samuel Gibbs, *The Guardian*, June 11, 2015.
149. Lemay et al. 2018.44–45.
150. https://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/.
151. https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/; Samuel Gibbs 2015, *The Guardian*, June 11, 2015; https://abcnews.go.com/Technology/duqu-20-invisible-cyber-espionage-tool-targeted-russian/story?id=31664104; Segal, A. *The Hacked World Order: How Nations Fight, Trade, Maneuver and*

Manipulate in the Digital Ages. New York: Public Affairs (2017), p.4; Rid, T. *Cyber War Will Not Take Place*. London: C. Hurst and Co (2013). p. 93.

152. Lemay et al. 2018.44–45; Samuel Gibbs, *The Guardian*, June 11, 2015.
153. Smeets 2017.24; Samuel Gibbs, *The Guardian*, June 11, 2015.
154. Sanger 2018.xiv; Heckman et al. 2015.56–58.
155. R. Sale, *Industrial Safety and Security Source*, April 11, 2012; M. B. Kelley, *Business Insider*, November 20, 2013; Wang et al. 2018.710.
156. For a detailed technical discussion of how Stuxnet worked, see: Barzashka 2013; Sanger 2018; Zetter 2014; Wang et al. 2018; Heckman et al. 2015; Cohen et al. 2016.
157. Sanger 2018.24; Joint Advanced Warfighting School 2014.14–15; Fulghum 2012; Farwell and Rohozinski 2011.25; Parmenter 2013.45–49; Zetter 2014; Sanger 2012; Fulghum 2010.29; Lemay et al. 2018.44–45; Heckman et al. 2015.56–58; Valeriano and Maness 2015.152; Rid 2013; Schmidt and Cohen 2014.105; Nourian and Madnick 2018.6.
158. Sanger 2012.174–191; Sanger 2018.24; Parmenter 2013.45, 49; Heckman et al. 2015.56–57; Valeriano and Maness 2015.152; Rid 2013; Schmidt and Cohen 2014.105.
159. Nourian and Madnick 2018.6; Heckman et al. 2015.56–57; Valeriano and Maness 2015.152; Rid 2013; Schmidt and Cohen 2014.105.
160. Sanger 2012.174–191; Sanger 2018.24; Parmenter 2013.45, 49; Heckman et al. 2015.56–57; Valeriano and Maness 2015.152; Rid 2013; Schmidt and Cohen 2014.105.
161. Zetter and Modderkolk 2019; Sanger 2018.21; Nissim et al. 2017; http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/.
162. Fulghum 2012; Farwell and Rohozinski 2011.25; Joint Advanced Warfighting School 2014.14; Parmenter 2013.45–49; Zetter 2014; Sanger 2012; Fulghum 2010.29; Rid 2013; Slayton 2016/2017; Sanger 2018. 24.
163. Rid 2013; Slayton 2016/2017.
164. Cohen et al. 2015.8; Heckman et al. 2015.58; Brantly 2018; Nourian and Madnick 2018.6.
165. Rid 2013; Buchanan 2017.75.
166. Sanger 2018.24; Rid 2013; Slayton 2016/2017; http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/; Nissim et al. 2017.683; Bahtiyar et al. 2019. 119; Harris 2014.96.
167. Rid 2013; Slayton 2016/2017.
168. Rid 2013; Slayton 2016/2017.
169. Smeets 2018.22; Anderson and Sadjadpour 2018.59.
170. Nourian and Madnick 2018.5–6.
171. Rid 2013; Slayton 2016/2017.
172. Bellovin et al. 2017.61.
173. Smeets 2018.22; Anderson and Sadjadpour 2018.59; Sanger 2018.25, 44.
174. David Sanger and Mark Mazzetti, *New York Times*, February 17, 2016.
175. Sanger 2018.23; Heckman et al. 2015.54–55; O'Connell 2015.519.
176. Sanger 2018.23.
177. Harris 2014.46–47; Boldizsár Bencsáth, "Duqu, Flame, Gauss: Followers of Stuxnet," BME CrySyS Lab, RSA Conference Europe 2012.
178. David Sanger and Mark Mazzetti, *New York Times*, February 17, 2016.
179. Sanger 2018.39, 42–44.
180. Sanger 2018.43–45; David Sanger and Mark Mazzetti, *New York Times*, February 17, 2016; Stockburger 2016.548, 559–560.
181. Stockburger 2016.548, 559–560.
182. Eric Schmitt and Julian Barnes, *New York Times*, May 13, 2019.
183. Egozi 2011.5; Sanger 2018.41; Harris 2014.46–47; Brantly 2018.60.
184. Smeets 2018.102; Sanger 2018.21.
185. Sanger 2018.21.
186. Zetter and Modderkolk 2019.
187. Smeets 2018.102; Sanger 2012. 275.
188. Jensen 2017.167–168; Valeriano and Maness 2015.155; Gartzke and Lindsay 2014.4.
189. Parmenter 2013.39–40, 42–43; Joint Advanced Warfighting School 2014.14–15; Sanger 2012; Cohen et al. 2016.

190. Slayton 2016/2017.104; David Sanger, *New York Times*, June 1, 2012; Farwell and Rohozinski 2012.111.
191. Barzashka 2013.48; Valeriano and Maness 2015.156; Lindsay 2013.369.
192. Barzashka 2013.48.
193. Sanger 2018.42; Barzashka 2013.48; Valeriano and Maness 2015.156; Lindsay 2013.369.
194. See Chapter 5.
195. Sanger 2018.22.
196. McGraw 2013.112; Sanger 2018.17, 32.
197. https://www.wired.com/story/russian-hackers-attack-ukraine/.
198. Sanger 2018.17; Parmenter 2013.39; Farwell and Rohozinski 2011.25.
199. https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.
200. https://www.timesofisrael.com/us-cyber attack-on-iran-exploited-flaw-in-heavily-guarded-network-experts-say/.
201. Carr 2012.51; Parmenter 2013.35–38; Fulghum 2012; Egozi 2011.6; Clarke and Knake 2012.4–6.
202. Tabansky in Cornish 2021.633.
203. Joby Warrick and Ellen Nakashima, *Washington Post*, May 18, 2020; Yonah Jeremy Bob, *Jerusalem Post*, May 19, 2020; Ronen Bergman and David Halbfinger, *New York Times*, May 19, 2020; Mehul Srivastav, *Financial Times*, May 31, 2020; Siman-Tov and Even 2020; TOI Staff, *Times of Israel*, July 17, 2020; Baram et al. 2021.
204. Amitai Ziv, *The Marker*, September 22, 2020; Yaakov Lappin and Jeremy Binnie, *Janes*, June 15, 2021; https://www.dw.com/en/israel-claims-hamas-was-using-bombed-ap-building-to-jam-iron-dome/a-57820377; https://www.portstrategy.com/news101/world/middle-east/cyberattack-prevented-on-irans-ports; https://www.intellinews.com/large-cyberatt ack-hit-iran-s-ports-electronic-infrastructure-194258/.
205. David Sanger, William Broad, Ronen Bergman, and Farnaz Fassihi, *New York Times*, July 2, 2020; David Sanger, Eric Schmidt, and Ronen Bergman, *New York Times*, July 10, 2020; TOI Staff and Agencies, *Times of Israel*, July 4, 2020; TOI Staff, *Times of Israel*, July 17, 2020; Judah Ari Gross, *Times of Israel*, July 3, 2020; Amos Harel, *Haaretz*, July 5, 2020; Jacky Houri, *Haaretz*, July 4, 2020; Yonah Jeremy Bob, *Jerusalem Post*, July 2, 2020; Simon Henderson, *The Hill*, July 6, 220.
206. Amos Harel, *Haaretz*, April 11, 2021; Ronan Bergman, Rick Gladstone, and Farnaz Fassihi, *New York Times*, April 11, 2021; Yaron Schneider, Nir Dvori, and Yaron Abraham, *N12*, April 11, 2021; Yonah Jeremy Bob, Lahav Harkov, and Tzvi Joffre, *Jerusalem Post*, April 12, 2021.
207. Farnaz Fassihi and Ronen Bergman, *New York Times*, June 23, 2021; https://nationalinterest.org/blog/middle-east-watch/what-forced-iran-shut-down-its-only-nuclear-power-plant-188428; https://www.reuters.com/world/middle-east/iran-restarts-bushehr-nuclear-power-plant-after-overhaul-state-media-2021-07-03/.
208. Tzvi Joffre, *Jerusalem Post*, August 22, 2021; *Reuters*, August 24, 2021.
209. Daniel Salame, *Ynet*, July 9, 2021; *Jerusalem Post* Staff, *Reuters*, July 11, 2021.
210. Ronen Bergman, *New York Times*, August 14, 2021.
211. Farnaz Fassihi and Ronen Bergman, *New York Times*, November 27. 2021.
212. Jeremy Yonah Bob, *Jerusalem Post*, November 21, 2021; *Ynet*, November 21, 2021; TOI Staff, *Times of Israel*, November 21, 2021.
213. *I24 News*, November 24, 2021; TOI Staff, *Times of Israel*, November 24, 2021.
214. *AP*, February 2, 2022; *Reuters*, January 27, 2022.
215. Amos Harel, *Haaretz*, June 29, 2022; Nina Fox, *YNet*, June 28, 2022; Isabel Debre, *Washington Post*, June 27, 2022.
216. Amos Harel, *Haaretz*, October 29, 2021; Zvi Barel, *Haaretz*, October 29, 2021; Yehonatan Lis, *Haaretz*, October 27, 2021; *YNet* and Agencies, October 27, 2021.
217. Yaron Schneider, Nir Dvori and Yaron Abraham, *N12*, April 11, 2021; Ron Ben Yishay, *YNet*, June 6, 2019; Amos Harel, *Haaretz*, April 11, 2021; Ronan Bergman, Rick Gladstone, and Farnaz Fassihi, *New York Times*, April 11, 2021.
218. David Sanger and Eric Schmitt, *New York Times*, June 12, 2017.
219. Yonah Jeremy Bob, *Jerusalem Post*, June 27, 2019.

220. Nicole Perlroth and Scott Shane, *New York Times*, October 10, 2017; Ellen Nakashima, *Washington Post*, October 10, 2017.
221. Egozi 2011.6.
222. Tal Shachaf, *YNet*, May 21, 2021; Nir Dvori, *N12*, May 19, 2021, and May 27, 2021; Amir Bochbot, Walla May 19, 2021; https://therecord.media/israel-bombed-two-hamas-cyber-targets/; https://www.securityweek.com/israel-says-its-fighter-jets-bombed-buildings-used-hamas-cyber-unit; https://www.bbc.com/news/world-middle-east-57404516.

Chapter 12

1. Ellsworth et al. 2000.16–17.
2. This definition of Israel's national security objectives draws heavily on the IDF Strategy 2018, as further elaborated by Freilich 2018.327–328.
3. State of Israel, Prime Minister's Office, the National Cyber Security Authority 2018.
4. IDF Strategy 2018.18, 21, 29.
5. Objective set by Prime Minister Netanyahu, Shoshana Solomon, *Times of Israel*, June 20, 2018.
6. Sanger 2018.17; US National Military Strategy for Cyber Operations quoted in Clarke and Knake 2010.44; Government of the United States, Department of Defense 2018.6, 9; Government of the United States, Department of Defense 2017.9; Government of the United States, Department of Defense 2018.4; Government of the United States, Department of Defense 2015b.7–8; Government of the United States, Department of Defense 2018.5.
7. Siboni and Assaf 2016.10.
8. Baldwin et al. 2012.
9. Baldwin et al. 2012.
10. https://www.inss.org.il/publication/establishing-an-idf-cyber-command/.
11. International Institute for Strategic Studies 2021.
12. Kehler in Lin and Zegart 2019.289–290, 293, 303–304.
13. Long in Lin and Zegart 2019.120–121.
14. Government of the United States 2020.101; Even 2015.
15. Government of the United States 2020.102.
16. Government of the United States 2020.101.
17. Government of the United Kingdom 2022.para 126.
18. Nir Zohar, *Haaretz*, April 1, 2021.
19. Jack Hennessey, *Jerusalem Post*, February 24, 2022.
20. Government of the United States 2020.77, 81; https://www.mobileye.com/he-il/.
21. Government of the United States, Department of Defense 2017.13–14.
22. Clarke and Knake 2010.176–178; Government of the United States 2020.25.
23. Sulmeyer 2018.
24. Freilich 2018.
25. See Chapter 10.
26. Government of Israel, State Comptroller 2022a.
27.. Government of the United States 2020.103; https://www.washingtonpost.com/politics/2021/09/24/congress-is-finally-going-big-cyber/.
28. Government of the United States 2020.57.
29. Siboni and Assaf 2016.64; Government of Israel, State Comptroller 2022.
30. For more on the technical aspects of this, see Fahrenkrug 2012.201; Applegate 2012.
31. Government of the United States, White House 2017.13.
32. Government of the United States 2020.82.
33. Government of Israel, State Comptroller 2022.
34. Government of the United States, Department of Defense 2015a.6; UK National Cybersecurity Strategy 2016–2021.33.
35. https://www.timesofisrael.com/superfast-sub-sea-internet-cable-to-connect-israel-with-spain/; Government of the United States, White House 2018.8; Eado Hecht, *JPost.com*, May 16, 2013.
36. International Institute for Strategic Studies 2021.
37. Shamir and Bachar 2019.12–14.

38. Government of Israel, State Comptroller 2022.1050.
39. Clarke and Knake 2010.176–178; Brantly 2018.114; NATO Parliamentary Assembly, Science and Technology Committee 2019.11; Jasper 2017.14; Siboni and Assaf 2016.79–81; Government of the United States, White House 2018; Government of the United States, Department of Defense 2018.1–2; UK National Cybersecurity Strategy, pp. 25, 33, 47.
40. Government of the United States, Department of Defense 2015b.14.
41. INCD National Cyber Strategy 2017.
42. Government of Israel, State Comptroller 2022.
43. Government of the United Kingdom 2022a; Government of the United Kingdom 2022b.
44. https://news.err.ee/988930/nine-more-nations-join-nato-cyberdefense-center; http://natoassociation.ca/the-internet-of-nato/; https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.
45. https://www.congress.gov/bill/113th-congress/house-bill/938.
46. https://www.defensenews.com/2015/12/13/israel-military-eyes-nato-like-global-cyber-coalition/; https://www.idc.ac.il/he/research/ips/pages/mabat/mabat-15-6-21.aspx.
47. https://www.timesofisrael.com/israel-entrepreneur-calls-for-nato-style-cybersecurity-alliance/.
48. Government of the United States 2020.116.
49. Buchanan 2017.168.
50. A possibility mooted by Nye 2016/2017.61.
51. Government of the United States, White House 2018.20; UK National Cybersecurity Strategy 2016–2021.49.
52. Buchanan 2017.166.
53. Ari Cicurel and Erielle Davidson, "After Biden-Bennett Meeting, Potential Israeli Action against Chinese Investments," NatSec Brfief, JINSA, September 14, 2021.
54. See Greenert and Bird 2021.52–64.

Appendix

1. " 'Anti-IS Group' Claims BBC Website Attack," *BBC*, January 2, 2016.
2. AppSec Knowledgebase, "Computer Worm," *Veracode*.
3. Kim Zetter, *Wired*, March 21, 2013.
4. Kaspersky Resource Center, "Trojan Horse," *Kaspersky*.
5. Allen Kim, *CNN*, October 8, 2019.
6. Allen Kim, *CNN*, October 8, 2019.
7. Nate Lord, *DataInsider*, July 17, 2020.
8. Milena Dimitrova, *Sensors*, March 8, 2016.
9. "What Is a 'Drive-By' Download?" *McAfee*, April 2, 2013.
10. "Watering Hole," *Symantec*.
11. A1:2017-Injection, *OWASP*.
12. "SQL Injection," *OWASP*.
13. "Eavesdropping," *Techopedia*.
14. "What Is Spoofing?" *Forcepoint*.
15. "Backdoor Computing Attacks," *Malwarebytes*.
16. "Cross-Site Scripting (XSS)," *Acunetix*.
17. "Keyloggers: How They Work and How to Detect Them (Part 1)," *SecureList*.
18. "Advanced Persistent Threat Groups," *Mandiant*.
19. "What Is a Zero-Day Exploit?" *Fireeye*.

BIBLIOGRAPHY

Ablon, L., Libicki, M., and Golay, A. "Markets for Cybercrime Tools and Stolen Data." Rand Corporation (2014).

Adamsky, D. "Israeli Culture of Innovation between Anticipation and Adaptation." *Bein Haktavim*, Dado Center, IDF (July 2019).

Adamsky, D. *The Culture of Military Innovation*. Stanford, CA: Stanford University Press (2010).

Adamsky, D. "The Israeli Odyssey toward Its National Cyber Security Strategy." *The Washington Quarterly*, 40, No. 2 (2017): 113–127.

Afek, S. "Breaking the Rules and Everybody Is Playing—on the Meeting between the Cybernetic Realm and International Law (Hebrew)." *Maarachot*, 3 (December 2014).

Anderson, C., and Sadjadpour, K. *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Washington, DC: Carnegie Endowment for International Peace (2018).

Antebi, L. "Artificial Intelligence and National Security in Israel (Hebrew)." INSS, Memorandum 205 (September 2020).

Applegate, S.D. "The Dawn of Kinetic Cyber." Fifth International Conference on Cyber Conflict. Tallinn, Estonia (2013).

Applegate, S.D. "The Principle of Maneuver in Cyber Operations." Fourth International Conference on Cyber Conflict. Tallinn, Estonia (2012).

Arad, U. "Grand Strategy for Israel (Hebrew)." Shmuel Neeman Institute, Haifa University (2017).

Argaman, S., and Siboni, G. "Commercial and Industrial Cyber Espionage in Israel." *Military and Strategic Affairs*, Institute for Strategic Studies, 6, No. 1 (2014): 43–58.

Arieli, I. *Chutzpah: Why Israel's a Hub of Innovation and Entrepreneurship*. New York: Harper (2019).

Australian Government. "Australia's Cybersecurity Strategy: Enabling Innovation, Growth and Prosperity, First Annual Update." Department of the Prime Minister and Cabinet (2017).

Australian Government. "Cyber Security Strategy." Attorney-General's Department (2009).

Australian Government. "Cyber Security Strategy 2020." Minister for Home Affairs (2020).

Bahtiyar, S., Yaman, M.B., and Altınigne, C.Y. "A Multi-Dimensional Machine Learning Approach to Predict Advanced Malware." *Computer Networks*, 160 (2019): 118–129.

Baldwin, R., et al. *Understanding Regulation: Theory, Strategy and Practice*. New York: Oxford University Press (2012).

Bar-Joseph, U. *Israeli National Security toward the 21st Century*. London: Frank Cass (2001).

Bar-Joseph, U. "The Crisis in Israel's Security Concept (Hebrew)." *Maarachot*, 401 (June 2005): 10–19.

Bar-Joseph, U. "The Paradox of Israeli Power." *Survival*, 46, No. 4 (2004–2005): 137–156.

Bar-Joseph, U. "Towards a Paradigm Shift in Israel's National Security Conception." *Israel Affairs*, 6, No. 3–4 (2000): 99–114.

Bar-Tal, D., Jacobson, D., and Klieman, A.S., eds. *Security Concerns: Insights from the Israeli Experience*. Stamford, CT: JAI Press (1998).

Baram, G., and Ben-Israel, I. "The Academic Reserve: Israel's Fast Track to High-Tech Success." *SSRN* (2018): https://ssrn.com/abstract=3269147; http://dx.doi.org/10.2139/ssrn.3269147.

Baram, G. "Israeli Defense in the Age of a Cyber War." *Middle East Quarterly* (Winter 2017): 1–10.

Baram, G. "The Effects of Cyber War Technologies on Force Buildup: The Israeli Case." *Military and Strategic Affairs*, 5, No. 1 (May 2013): 23–43.

Baram, G., and Ben-Israel, I. "The Academic Reserve: Israel's Fast Track to High-Tech Success." *Israel Studies Review*, 34, No. 2 (November 2018): 75–91.

Baram, G., Ram, Y., and Ben-Israel, I. *Cyberwar between Iran and Israel Out in the Open*. Tel Aviv University (January 2021). https://en-sectech.tau.ac.il/sites/bog.tau.ac.il/files/bog/Cyberwar%20Between%20Iran%20and%20Israel%20Out%20in%20the%20Open_Final_5.1.21.pdf.

Barak Ravid. "Netanyahu Formed a Team to Prepare for Israeli Attacks on Computer Networks." *Haaretz (Hebrew)*, April 3, 2011. http://www.haaretz.co.il/captain/software/1.1170180.

Barzashka, I. "Are Cyber-Weapons Effective?" *The RUSI Journal*, 158, No. 2 (2013): 48–56.

Bates, N. "Comparing Cyber Weapons to Traditional Weapons through the Lens of Business Strategy Frameworks." Information Security Group, Royal Holloway University of London (August 2020).

Bebber, R. "Information War and Rethinking Phase 0." *Journal of Information Warfare*, 15, No. 2 (2016): 39–52.

Bellovin, S.M., Landau, S., and Lin, H.S. "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications." *Journal of Cybersecurity*, 3, No. 1 (2017): 59–68.

Ben-David, A. "Playing Defense." *Aviation Week and Space Technology*, 173 (2011): 57.

Ben-Horin, Y., and Barry Posin. "Israel's Strategic Doctrine." *Rand Corporation* (September 1981).

Ben-Israel, I. *Israel Defense Doctrine* (Hebrew). Modan: Ben Shemen (2013).

Ben-Israel, I. "The Cyber Revolution in the Next Step: Intelligence Systems." *Swiss Cognitive* (June 2020). https://swisscognitive.ch/2020/06/26/prof_isaac_ben_israel_cognitivenations_israel/.

Ben-Moshe, N. "Chinese Espionage Operations in the United States: And in Israel?" *INSS Insight*, No. 1560 (February 20, 2022). https://www.inss.org.il/publication/china-espionage/.

Benoliel, D. "Towards a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study." *North Carolina Journal of Law and Technology*, 16, No. 3 (2015): 435–486.

Blank, Laurie R. "International Law and Cyber Threats from Non-State Actors." *US Naval War College*, 89 (2013): 406–437.

Blechman, B. *Unblocking the Road to Global Zero: Pakistan and Israel*. Washington, DC: Stimson Center (2011).

Borghard, E.D., and Lonergan, S.W. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly*, 13, No. 3 (2019): 122–145.

Bowden, M. *Worm: The First Digital War*. New York: Atlantic Monthly Press (2011).

Brantly, A.F. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia (2018).

Bren, D., and Levy, Y. "The ISIS Phenomenon—What the West Doesn't Understand." *Bein Haktavim* (Hebrew), 3 (2014): 111–138.

Breznitz, D. *The Military as a Public Space: The Role of the IDF in the Israeli Software Innovation System*. Haifa: Samuel Neeman Institute, Technion (n.d.).

Brun, I. "Where Did Maneuver Disappear To? (Hebrew)." *Maarachot*, 420, No. 421 (September 2008): 4–15.

Brunner, J.A. "The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency." *Jurimetrics Journal* 57 (2017): 397–431.

Brom, S., ed. "Following Operation 'Defensive Pillar': Gaza Strip, November 2012 (Hebrew)." INSS Memorandum 123 (December 2012).

Brom, S., and Kurz, A., eds. *Strategic Assessment for Israel 2013–2014* (Hebrew). Tel Aviv: INSS (2014).

Brown, C.S., and Friedman, D. "A Cyber Chemical Convention? Lessons from the Conventions on Chemical and Biological Weapons." In *Arms Control and National Security: New Horizons*, ed. Emily B. Landau and Anat Kurz. Memorandum No. 135. Tel Aviv: Institute for National Security Studies (2014): 45–63.

Buchanan, B. *The Cyber Security Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford University Press (2017).

Bussolati, N. "The Rise of Non-State Actors in Cyberwarfare." In *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Clair Finkelstein. London: Oxford University Press (2015): 102–126.

Byman, D. *A High Price: The Triumphs and Failures of Israeli Counterterrorism*. Oxford: Oxford University Press (2011).

Çahmutoglu, E. *Iran's Cyber Power*. iRAM Report (April 2021).

Carr, J. *Inside Cyber Warfare*. Cambridge, UK: O'Reilly (2012).

Catignani, S. *Israeli Counterinsurgency and the Intifada: Dilemmas of a Conventional Army*. London: Routledge (2008).

Chachko, E. *Persistent Aggrandizement? Israel's Cyber Defense Architecture*. Aegis Series Paper 2002, Hoover Institution, Stanford University (August 26, 2020).

Charlet, K. *Understanding Federal Cybersecurity*. Cambridge, MA: Belfer Center, Harvard Kennedy School (April 2018).

Chen, J. "On Levels of Deterrence in the Cyber Domain." *Journal of Information Warfare*, 17, No. 2 (2018): 32–41.

Cherry, S. "Terror Goes Online." *IEEE Spectrum*, 42, No. 1 (2005): 72–73.

Cherry, S. "The Net Effect." *IEEE Spectrum*, 42, No. 1 (2005): 72–73.

Chong, A. "Information Warfare?: The Case for an Asian Perspective on Information Operations." *Armed Forces & Society*, 40, No. 4 (2014): 599–624.

Chorev, M. *"Deterrence Campaigns": Lessons from IDF Operations in Gaza* (Hebrew). Studies in Middle Eastern Security 115. Ramat Gan: BESA 2015: 1–65.

Choucri, N. *Cyberpolitics and International Relations*. Cambridge, MA: MIT Press (2012).

Cilluffo, F., Cardash, S.L., and Salmoiraghi, G.C. "A Blueprint for Cyber Deterrence: Building Stability through Strength." *Institute for National Security Studies, Military and Strategic Affairs*, 4, No. 3 (2012): 3–23.

Cilluffo, F., and Clark, J.R. "Building a Conceptual Framework for Cyber's Effect on National Security." *Journal of Information Warfare*, 15, No. 2 (2016): 1–16.

Clarke, R.A., and Knake, R.K. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins (2010).

ClearSky Research Team. "Operation Dusty Sky—Part 2." Clearsky Cybersecurity (2016).

ClearSky Research Team. "Operation Wilted Tulip—Exposing a Cyber Espionage Apparatus." *Clearsky Cybersecurity* (2017).

ClearSky Research Team. "Thamar Reservoir—An Iranian Cyber-Attack Campaign against Targets in the Middle East." Clearsky Cybersecurity (2015).

Cohen, D., and Levin, D. "Operation Protective Edge: The Cyber Defense." In *The Lessons of Operation Protective Edge*, ed. Anat Kurz and Sholmo Brom. Institute for National Security Studies (2014a): 59–63. inss.org.il/publication/the-lessons-of-operation-protective-edge/.

Cohen, D., and Levin, D. "SEA: How Real Is the Threat?" *INSS Insight*, No. 521 (2014b). https://i-hls.com/archives/28919.

Cohen, D., and Rotbart, A. "The Proliferation of Weapons in Cyberspace." In *Cyberspace and National Security—Selected Articles*, ed. Gabi Siboni. Institute for National Security Studies (2013): 105–125. https://www.inss.org.il/publication/cyberspace-and-national-security-selected-articles/.

Cohen, E., Eisenstadt, M., and Bacevich, A. "Knives, Tanks and Missiles: Israel Security Revolution." *Washington Institute for Near East Policy* (1998). https://www.washingtoninstitute.org/media/3594.

Cohen, M.S., Freilich, C.D., and Siboni, G. "Israel and Cyberspace: Unique Threat and Response." *International Studies Perspectives*, 17, No. 3 (August 2016): 307–321.

Cohen, M.S., Freilich, C.D., and Siboni, D. "Four Big 'Ds' and a Little 'r': A New Model for Cyber Defense." *Cyber, Intelligence, and Security*, 1, No. 1 (2017): 21–36.

Cohen, N. "Israeli Preparations for a Broad Cyber Attack." *Maarachot*, 452 (December 2013): 10–17.

Cohen, R. "Israel's Starry-Eyed Foreign Policy." *Middle East Quarterly*, 1, No. 2 (1991): 28–41.

Cohen, S., and Klieman, A. *Routledge Handbook on Israeli Security*. New York: Routledge (2019).

Collin, B. *The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge*. Proceedings of 11th Annual International Symposium on Criminal Justice Issues. Chicago: University of Illinois. (2016).

Colonel A., et al. "Towards Military Superiority in The Cyber Dimension." *Bein Haktzvim*, 28, No. 30 (2020): 149–163.

Conti, G., and Raymond, D. *On Cyber: Towards an Operational Art for Cyber Conflict*. New York: Kopidion (2017).

Cooper, J. "A New Framework for Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron. Washington, DC: Georgetown University Press (2012a): 105–120.

Corn, G., and Jensen, E. "The Use of Force and Cyber Countermeasures." *Temple International & Comparative Law Journal*, 32, No. 2 (2018): 127–134.

Cornish, P., ed. *Oxford Handbook of Cybersecurity*. Oxford: Oxford University Press (2021).

Crosston, Matthew. "Duqu's Dilemma: The Ambiguity Assertion and the Futility of Sanitized Cyberwar." *Military and Strategic Affairs*, 5, No. 1 (2013): 119–131.

Dagan, O., and Bar-Lev, L. "Stopping at Delphi on the Route the Digital Supremacy." *Bein Haktavim* (Hebrew), 28, No. 30 (2020): 163–194.

Danino, O. "An Overview of Israeli Efforts in the Cybernetics Field." *Israel National Cyber Bureau (INCB)*, 3, No. 21 (March 2015). https://www.chaire-cyber.fr/IMG/pdf/tr_article_3_21_-_chaire_cyberdefenseeng.pdf.

Davis, J.S., Boudreaux, B., Welburn, J., Aguirre, J., Ogletree, C., McGovern, G., and Chase, M.S. *Stateless Attribution: Toward International Accountability in Cyberspace*. Santa Monica, CA: RAND Corporation (2017).

Deibert, R., and Rohozinski, R. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology*, 4, No. 1 (2010): 15–32.

Dekek, U., and Einav, O. "An Updated National Security Strategy for Israel." INSS, Special Memorandum (2017).

Demchak, C. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron. Washington, DC: Georgetown University Press (2012a): 121–136.

Demchak, C. "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)." *Journal of Comparative Policy Analysis*, 14, No. 3 (2012b): 254–269.

Demchak, C. *Wars of Disruption and Resilience*. Athens: University of Georgia Press (2011).

Demchak, C., and Dombrowski, P. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly,* 1 (2011): 32–61.

Denning, D. "Cyberterrorism." Proceedings of Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives. Washington, DC (May 23, 2000).

DeVore, M.R., and Lee, S. "APT (Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict." *The Journal of East Asian Affairs*, 31, No. 1 (2017): 39–64.

Dolev, B., and Siman-Tov, D. "Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks." *INSS*, Special Publication (January 27, 2022).

Dombowski, M., and IronNet Threat Research and Intelligence Teams. "Analysis of the Iranian Cyber Attack Landscape." *IronNet* (September 14, 2021). https://www.ironnet.com/blog/iranian-cyber-attack-updates.

Donnelly, D.A., Clements, S.L., and Goychayev, R. "A Technical and Policy Toolkit for Cyber Deterrence and Stability." *Journal of Information Warfare*, 18, No. 3 (2019): 53–69.

Dror, Y. *Israeli Statecraft: National Security Challenges and Responses*. London: Routledge (2011).

Egozi, A. "The Secret Cyber War." *Military Technology*, 35 (2011): 5–6.

Eichensher, K. "Cyberwar & International Law Step Zero." *Texas International Law Journal*, 50, Symposium 2 (2015): 355–378.

Eilstrup-Sangiovanni, M., "Why the World Needs an International Cyberwar Convention." *Philosophy & Technology*, 31 (2018): 379–407.

Eisenkot, G. "Cyber in the IDF." *Cyber, Intelligence and Defense*, 2, No. 3 (2018): 91–95.

Eisenkot, G., and Siboni, G. "Guidelines for Israel's National Security Strategy." Policy Focus 160, Washington Institute for Near East Policy (October 2019).

Eisenstadt, M., and D. Pollock. "How the United States Benefits from Its Alliance with Israel." Strategic Report 7, *The Washington Institute for Near East Public Policy* (September 2012).

Ellsworth, R, Goodpaster, A., and Hauser, R. Co-Chairs. "America's National Interests: A Report from the Commission on America's National Interests, 2000." Commission on America's National Interests (2000).

Elran. M., Shaham, Y., and Altshuler, A. "An Expanded Comprehensive Threat Scenario for the Home Front in Israel." *INSS Insight*, 828 (June 2016a).

Elran. M., Shaham, Y., and Altshuler, A. *IDF Strategy in the Perspective of National Security*. INSS (2016b).

Eriksson, J., and Giacomello, G. "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review*, 27, No. 3 (2006): 221–244.

European Commission. High Representatives of the European Union for Foreign Affairs and Security Policy. "Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace." Brussels (February 7, 2013).

Even, S. "The Strategy for Integrating the Private Sector in National Cyber Defense in Israel." *Military and Strategic Affairs*, 7, No. 2 (September 2015): 113–114.

Even, S., and Siman-Tov, D. "Cyber Warfare: Concepts and Strategic Trends." Memorandum No. 117. Institute for National Security Studies (2012).

Even, S., Siman-Tov, D., and Siboni, G. "Structuring Israel's Cyber Defense." *INSS Insight*, No. 856 (September 21, 2016).

Fahrenkrug, D.T. *"Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy."* 4th International Conference on Cyber Conflict, Tallinn (2012).

Fanelli, R. "Cyberspace Offense and Defense." *Journal of Information Warfare*, 15, No. 2 (2016): 53–65.

Farwell, J.P., and Rohozinski, R. "Stuxnet and the Future of Cyber War." *Survival*, 53, No. 1 (2011): 23–40.

Farwell, J.P., and Rohozinski, R. "The New Reality of Cyber War." *Survival*, 54, No. 4 (2012): 107–120.

Feldman, S., and Toukan, A. *Bridging the Gap: A Future Security Architecture for the Middle East*. New York: Carnegie (1997).

Finkel, M. "The Gideon Five-Year Plan in Comparison with Developments in Foreign Armies." *Maarachot*, 471 (May 2017): 13–16.

Finnemore, M. *National Interests in International Society*. Ithaca, NY: Cornell University Press (1996).

Finnemore, M., and Hollis, D. "Constructing Norms for Global Cyber-Security." *American Journal of International Law*, 110, No. 3 (2016): 425–479.

Fischerkeller, M.P., and Harknett, R.J. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis*, 61, No. 3 (2017): 381–393.

Fischerkeller, M.P., and Harknett, R.J. "What Is Agreed Competition in Cyberspace?" *Lawfare* blog (February 19, 2019).

Foradori, P., and Malin, M.B., eds. *A WMD Free Zone in the Middle East: Regional Perspectives*. Discussion Paper 2013–09, Belfer Center, Harvard Kennedy School (2013).

Frei, J. *Israel's National Cyber Security and Cyber Defense Posture: Policy and Organizations*. Zürich: Center for Security Studies (September 2020).

Freilich, C.D. *Zion's Dilemmas: How Israel Makes National Security Policy*. Ithaca: Cornell University Press (2012).

Freilich, C.D. "Israel: National Security Decision-Making in a Leaky Political Fishbowl." *Comparative Strategy*, 34, No. 2 (2015): 117–132.

Freilich, C.D. "National Security Decision-Making in Israel: Improving the Process." *Middle East Journal*, 67, No. 2 (2013): 257–266.

Freilich, C.D. "National Security Decision Making in Israel: Processes and Pathologies." *Middle East Journal*, 60, No. 4 (2006): 635–663.

Freilich, C.D. *Israeli National Security: A New Strategy for an Era of Change*. New York: Oxford University Press (2018).

Freilich, C.D. *The Armageddon Scenario: Israel and the Threat of Nuclear Terrorism*. Mideast Security and Policy Studies #84, Begin-Sadat Center (2010).

Freilich, C.D. "Why Can't Israel Win Wars Any More?" *Survival*, 57, No. 2 (2015): 79–92.

Freilich, C.D. *Zion's Dilemmas: How Israel Makes National Security Policy*. Ithaca, NY: Cornell University Press (2012).

Fulghum, D. "Bombing Iran." *Aviation Week and Space Technology*, 174, No. 22 (2012): 29.

Fulghum, D. "No Fingerprints." *Aviation Week and Space Technology*, 172, No. 36 (2010): 29.

Ganor, B. *The Counter-Terrorism Puzzle, A Guide for Decision Makers*. New Brunswick, NJ: Transaction (2005).

Garcia, Denise. "Killer Robots: Why the US Should Lead the Ban." *Global Policy*, 6, No. 1 (2015): 57–63.

Gartzke, E. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security*, 38, No. 2 (2013): 41–73.

Gartzke, E., and Lindsay, J.R. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. University of California, San Diego (2014). https://quote.ucsd.edu/deterrence/files/2014/12/EGLindsay_CDDOverview_20140715.pdf.

Gartzke, E., and Lindsay, J.R. "Thermonuclear Cyberwar." *Journal of Cybersecurity*, 1, No. 3 (2017): 37–48.

Geers, K. *Strategic Cyber Security*. Tallinn, Estonia: CCD COE Publication (2011).

Gelber, Y. "The Defense Doctrine and Place of the Army in Israeli Society." Policy Paper #3. Policy and Strategy Institute, Herzlia (May 2014).

Goines, T.M. "Overcoming the Cyber Weapons Paradox." *Strategic Studies Quarterly*, 11, No. 4 (2017): 86–111.

Golan, Y. "New Thinking about Israeli National Security in a Changing Regional Environment." Zeev Schiff Memorial Lecture. The Washington Institute for Near East Policy (September 7, 2017). https://www.washingtoninstitute.org/policy-analysis/new-thinking-about-israeli-national-security-changing-regional-environment.

Goldschmidt, R. "Arranging Responsibility for Governmental and Public Institution Cyber-Defense." *Knesset Research Service* (March 8, 2017). https://fs.knesset.gov.il/globaldocs/MMM/6d7a8b89-eef8-e611-80ca-00155d020699/2_6d7a8b89-eef8-e611-80ca-00155d020699_11_8242.pdf.

Government of France. "French National Digital Security Strategy." Agence Nationale de la Securite des Systemes d'Information (ANSSI) (October 16, 2015).

Government of Israel, Cabinet Secretariat. "Cabinet Decision 2443 Promoting National Regulation and Governmental Leadership in Cyber Defense." (February 15, 2015a).

Government of Israel, Cabinet Secretariat. "Cabinet Decision 2444, Promoting National Preparation for Cyber Defense." (February 15, 2015b).

Government of Israel, Supervisor of Banks. "Cyber Security Management." (2015).
Government of Israel, Israel Innovation Authority. "State of Innovation in Israel 2021." (2021).
Government of Israel, Israel Ministry of Foreign Affairs. "Deputy FM Elkin: Israel's Cyber Security." Address to the Seoul Conference on Cyberspace (October 16, 2013).
Government of Israel, Knesset, Foreign and Defense Affairs Committee, Subcommittee on Cyber-Defense. "Assessment of the Division of Responsibility and Authority in the Field of Cyber-Defense in Israel, Unclassified Report." (August 2016).
Government of Israel, Office of the Chief of Staff. "IDF Strategy." (2015). https://www.inss.org.il/he/wp-content/uploads/sites/2/2017/04/IDF-Strategy.pdf.
Government of Israel, Prime Minister's Office. "Australia Israel Joint Statement." (February 23, 2017).
Government of Israel, Prime Minister's Office. "Decision 3611." (2011).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Annual Report (Hebrew)." (2019).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Annual Report (Hebrew)." (2020).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Annual Report (Hebrew)." (2021).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "CERT-IL—Operational Principles for Addressing Cyber Threats (Hebrew)." (2015).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Cyber Defense Methodology for an Organization (Hebrew)." Ver. 1.0 (2017a).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Israel's National Cyber Security Strategy (Hebrew and English executive summary)." (2017b).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "National Cyber Concept for Crisis Preparedness and Management (Hebrew)." (2018).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Summary of the Founding Years 2016–2017 (Hebrew)." (2017c).
Government of Israel, Prime Minister's Office, National Cyber Directorate. "Use of Cloud Services: Addendum to the Organizational Cybersecurity Methodology (Hebrew)." (2017d).
Government of Israel, State Comptroller. "Report: Cybersecurity in Israel Electric Corporation (Hebrew)." (March 2022a).
Government of Israel, State Comptroller. "Report: Information Systems and Cyber Security in the Elections to the 21st, 22nd and 23rd Knessets (Hebrew)." (March 2022b).
Government of Israel, State Comptroller. "State Comptroller, Report 67A (Hebrew)." (2016).
Government of Israel, State Comptroller. "State Comptroller, Report 69B" (2019).
Government of Israel, Prime Minister's Office, the National Cyber Security Authority. "Draft Cyber Defense Legislation and National Cyber Authority 2018 (Hebrew)." (2018).
Government of Israel, Prime Minister's Office, the National Cyber Security Authority. "Israel's Cyber Defense Strategy (Hebrew)." (2017).
Government of the United Kingdom. "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy." (March 2021).
Government of the United Kingdom. "Government Cyber Security Strategy: Building a Cyber Resilient Public Sector 2022–2030." (January 25, 2022a).
Government of the United Kingdom. "National Cyber Security Strategy 2016–2021." (November 1, 2016). https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
Government of the United Kingdom. "National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK." (February 7, 2022b).
Government of the United Kingdom, National Cyber Security Center. "Advisory: APT29 Targets Covid-19 Vaccine Development." (2020).
Government of the United Kingdom, Parliament. "National Security Strategy." (2021).

Government of the United Kingdom, UK Cabinet Office. "Israeli and UK Academics to Combat Global Cyber Security Threats." The Rt Hon Lord Maude of Horsham and Government Digital Service (March 24, 2015).

Government of the United States. "Cyberspace Solarium Commission" (March 2020).

Government of the United States, Congressional Research Service. "Iranian Offensive Cyber Attack Capabilities." (January 13, 2020).

Government of the United States, Department of Defense, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. "Task Force on Cyber Deterrence." (February 2017).

Government of the United States, Department of Defense, US Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Version for US Cyber Command." (June 2018).

Government of the United States, Department of Defense, US Cyber Command. "Cyberspace Strategy Symposium Proceedings." (2018).

Government of the United States, Department of Defense. "Special Report: Cyber Strategy." (2015a).

Government of the United States, Department of Defense. "Summary of the National Defense Strategy." (2018).

Government of the United States, Department of Defense. "The DoD Cyber Strategy." (2015b).

Government of the United States, Department of Homeland Security. "Cybersecurity Strategy." (2018).

Government of the United States, Director of National Intelligence. "Annual Threat Assessment." (2021).

Government of the United States, National Intelligence Council. "Foreign Threats to the 2020 Federal Elections." (March 10, 2021).

Government of the United States, Office of the Under Secretary of Defense for Acquisition: Technology and Logistics. "Task Force on Cyber Deterrence." (February 2017).

Government of the United States, Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. "Cyber Incident Response." (2014).

Government of the United States, United States Department of Justice. "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." (March 23, 2018).

Government of the United States, White House. "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World." (May 2011).

Government of the United States, White House. "National Cyber Strategy of the United States." (2018).

Government of the United States, White House. "National Security Strategy of the United States." (December 2017).

Government of the United States, White House. "National Security Strategy of the United States." (September 2018).

Government of the United States, White House. "National Strategy for Combating Terrorism." (2003).

Government of the United States, White House Office of the President. "The National Strategy to Secure Cyberspace." (2003).

Graumann, B. *The Vexed Question of Global Rules. An Independent Report of Cyber-Preparedness around the World*. Brussels: Security and Defense Agenda (2013).

Greenert, J.W., and Bird, J.M. "Countering Chinese Engagement with Israel: A Comprehensive and Cooperative US-Israeli Strategy." Jewish Institute for National Security Affairs (JINSA), Washington DC (2021).

Greenhouse, Z., and Barros, G. "The Kremlin Leverages Cyber Cooperation Deals." *Institute for the Study of War* (2020): 1–4. https://www.jstor.org/stable/resrep29380?seq=4#metadata_info_tab_contents.

Groll, E. "Cyberattack Targets Safety System at Saudi Aramco." *Foreign Policy* (December 21, 2017). https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/.

Groll, E. "The Future Is Here and It Features Hackers Getting Bombed." *Foreign Policy* (May 6, 2019). https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Gupta, A. "Modi in Israel: Diplomacy and Development." BESA Center Perspectives Paper, No. 547 (2017).

Handel, M.I. *Israel's Political-Military Doctrine*. Cambridge, MA: Harvard University Press (1973).

Hansen, L., and Nissenbaum, H. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53, No. 4 (2009): 1155–1173.

Harknett. R.J. "United States Cyber Command's New Vision: What It Entails and Why It Matters." *Lawfare* blog (March 23, 2018).

Harknett, R.J., and Goldman, E.O. "The Search for Cyber Fundamentals." *Journal of Information Warfare*, 15, No. 2 (2016): 81–88.

Harris, S. *@War: The Rise of the Military-Internet Complex*. New York: Mariner (2014).

Hatch, B.B. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." *Journal of Strategic Security*, 11, No. 1 (2018): 43–61.

Hathaway, O., Crootof, R., Levitz, P., and Nix, H. "The Law of Cyber-Attack." *California Law Review*, 100, No. 4 (2011): 817–885.

Healey, J. "Getting the Drop in Cyberspace." *Lawfare* blog (August 19, 2019a).

Healey, J. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity*, 5, No. 1 (2019b): 1–15.

Heckman, K., Stech, F., Thomas, R., Schmoker, B., and Tsow A. *Cyber Denial, Deception and Counter Deception*. New York: Springer (2015).

Heller, M.A. *Continuity and Change in Israeli Security Policy*. Adelphi Paper 335. Oxford: Oxford University Press (2000).

Henning, L.A. *Encyclopedia of Cyber Warfare.* Edited by Springer, P. Denver, Colorado: ABC-CLIO (2017).

Herr, T. *PrEP: A Framework for Malware & Cyber Weapons*. Cyber Security Policy and Research Institute, George Washington University (March 12, 2014).

Hiddai, S. "Looking towards 6G: Israel and the Age of Technological Decoupling." *INSS Insight*, 1403 (November 18, 2020).

Hirshoga, Or, and Nati Toker, "Cyber Battles against Israel." *The Marker (Hebrew)* (November 22, 2012). http://www.themarker.com/technation/1.1871058.

House of Representatives Joint Hearing, *Cyber Incident Response: Bridging the Gap between Cybersecurity and Emergency Management*, Subcommittee on Emergency Preparedness, Response, and Communications and the Subcommittee on Cybersecrity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, 113th Congress Serial No. 113-39, October 30, 2013.

Housen-Couriel, D. "A Look at Israel's New Draft Cyber Security Law." *Council on Foreign Relations* (July 2, 2018). https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law.

Housen-Couriel, D. "National Cyber Security Organization: Israel." *NATO Cooperative Cyber Defense Center of Excellence*, 2, No. 4 (2017): 1–21.

Housen-Couriel, D. "The Evolving Law and Cyber Terrorism." *International Counterterrorism Review*, 1, No. 1 (2020): 1–28.

Housen-Couriel, D., Mimran, T., and Shany, Y. "Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill." *Lawfare* blog (May 7, 2021).

Hurwitz, R. "The Play of States: Norms and Security in Cyberspace." *The Journal of the National Committee on American Foreign Policy*, 36, No. 5 (2014): 322–331.

IISS. "Cyber Capabilities and National Power: A Net Assessment." (June 28, 2021). https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

Inbar, E. "Jews, Jewishness and Israel's Foreign Policy." *Jewish Political Science Review*, 2, No. 3–4 (1990): 29–50.

Inbar, E. *Israel's National Security: Issues and Challenges Since the Yom Kippur War*. London: Routledge (2008).

Inbar, E., and Shamir, E. "'Mowing the Grass'—Israel's Strategy for Coping with Ongoing and Unsolvable Crises (Hebrew)." Studies in Middle Eastern Security #105, BESA, Ramat Gan (December 2013).

INCD National Cyber Strategy. "Israel National Cyber Security Strategy in Brief." (September 2017).

Inserra, D., and Bucci, S.P. "Cyber Supply Chain Security: A Crucial Step toward U.S. Security, Prosperity, and Freedom in Cyberspace." Backgrounder #2880, The Heritage Foundation (March 6, 2014).

Institute for National Security Studies. "Global Cyber Bi-Weekly Report." (May 1, 2016).

Institute for National Security Studies. "Global Cyber Bi-Weekly Report." (September 1, 2016).

Institute for National Security Studies and the Cyber Security Forum Initiative. *INSS Insight* 598 (2014a). https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20598%20-%20Gabi%20and%20Sami%20for%20web.pdf.

Institute for National Security Studies and The Cyber Security Forum Initiative. "Cyber Intelligence Report." (July 15, 2014b).

International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment." Research Papers (June 28, 2021).

Isnarti, R. "A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War." *Andalas Journal of International Studies*, 5, No. 2 (2016): 151–165.

Israel Intelligence Heritage and Commemoration Center, Institute for Intelligence Methodology Research. *Leadership under Fire from Jointness: Jointness, People and What Is between Them*. By R, deputy head of the ISA. (April 4, 2021).

Jasper, S. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. New York: Rowman and Littlefield (2017).

Jensen, B.M. "The Cyber Character of Political Warfare." *Brown Journal of World Affairs*, 24, No. 1 (Fall/Winter 2017): 159–171.

Jensen, B.M., and Valeriano, B. "What Do We Know about Cyber Escalation? Observations from Simulations and Surveys." Issue Brief, Atlantic Council (2019).

Jervis, R. "Cooperation Under the Security Dilemma." *World Politics*, 30, No. 2 (January 1978): 167–214.

Jervis, R. "Some Thoughts on Deterrence in the Cyber Era." *Journal of Information Warfare*, 15, No. 2 (2016): 66–73.

Joint Advanced Warfighting School. "Nothing New Under the Sun: Benefiting from the Great Lessons of History to Develop a Coherent Cyberspace Deterrence Strategy." CreateSpace Independent Publishing Platform (April 8, 2014).

Jones, C., and Catignani, S., eds. *Israel and Hezbollah: An Asymmetrical Conflict in Historical and Comparative Perspective*. London: Routledge (2010).

Jorisch, A. *Thou Shalt Innovate: How Israel Ingenuity Repairs the World*. Jerusalem: Gefen Publishing (2018).

Kahane, B. "'Tikun Olam': How a Jewish Ethos Tries Innovation." *Journal of Management Development*, 31, No. 9 (2012): 938–946.

Kahn, L. *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*. Edited by Allhoff, F., Evans, N.G., and Henschke, A. New York: Routledge (2013).

Katzir, R. "By Sea, Air and Ground, and by Cyber?" *Maarachot*, 4 (2015): 103–119.

Kausch, K., and Tabansky, L. "Cybered Conflict in the Middle East." *Mediterranean Dialogue Series*, Mediterranean Advisory Group, 15 (April 2018): 1–11.

Keck, M.E., and Sikkink, K. *Activists beyond Borders: Advocacy Networks in International Politics.* Ithaca, NY: Cornell University Press (1998).

Kello, L. "The Meaning of the Cyber Revolution." *International Security*, 38, No. 2 (Fall 2013): 23–26.

Kenney, M. "Cyber-Terrorism in a Post-Stuxnet World." *Orbis*, 59, No. 1 (2015): 111–128.

Khazan, Olga. "Anonymous Is Hacking Israeli Web Sites." *Washington Post*, November 17, 2012, http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/17/anonymous-is-hacking-israeli-web-sites/.

Kissinger, H. *World Order*. New York: Penguin Press (2014).

Klein, J.J. "Deterring and Dissuading Cyberterrorism." *ASPJ Africa & Francophonie*, No. 1 (2018): 21–34.

Klieman, A.S. *Israel and the World after Forty Years*. Washington: Pergamon-Brassey (1990).

Kober, A. *Israel's Wars of Attrition: Attrition Challenges to Democratic States*. London: Routledge (2009).

Kober, A. *Military Decision in the Arab-Israeli Wars 1948–1982* (Hebrew). Tel Aviv: Maarachot Press (1995).

Koh, H.H. "The Emerging Law of 21st Century War: Keynote Address to the Emory Law School 2016 Randolph W. Thrower Symposium, Redefined National Security Threats: Tensions and Legal Implications." *Emory Law Journal*, 66, No. 487 (2017): 487–512.

Kreps, S., and Schneider, J. "Escalation Firebreaks in the Cyber, Conventional and Nuclear Domains: Moving beyond Effects-Based Logics." *Journal of Cybersecurity*, 5, No. 1 (2019): 1–11.

Kuehl, D. "Cyberspace and Cyberpower." In *Cyberpower and National Security*, ed. F.D. Kramer, S. Starr, and L. Wentz. Washington, DC: National Defense University Press (2009): 24–42.

Kugler, R. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, ed. F.D. Kramer. Washington, DC: National Defense University Press and Potomac Books (2009): 309–341.

Kuperwasser, Y., and Siman-Tov, D., eds. "The Cognitive Campaign: Strategic and Intelligence Perspectives." Memorandum 197, INSS (2019).

Kushner, D. "The Real Story of Stuxnet." *IEEE Spectrum*, 50, No. 3 (2013). http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Landau, E.B. *Arms Control in the Middle East: Cooperative Security Dialogue and Regional Constraints*. Brighton, UK: Sussex Academic Press (2006).

Landau, E.B. "Israel's Nuclear Ambiguity, Arms Control Policy, and Iran: Is the Time Ripe for Basic Changes?" *INSS Insight*, No. 478 (2013). https://www.inss.org.il/publication/israels-nuclear-ambiguity-arms-control-policy-and-iran-is-the-time-ripe-for-basic-changes/.

Landau, E.B., and Bermant, A., eds. *The Nuclear Nonproliferation Regime at a Crossroads*. Memorandum 137, INSS (May 2014).

Lemay, A., Calvet, J., Menet, F., and Fernandez, J.M. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors." *Computers & Security*, 72 (2018). 26–59.

Leved, L. "The Minotaur's Maze or: The Cyber Paradox—a Systemic Analysis of the Challenges and Opportunities in the Online Realm (Hebrew)." *Maarachot*, 3 (December 2014): 77–110.

Levite, A. "Global Zero: An Israeli Vision of Realistic Idealism." *Washington Quarterly,* 33, No. 2 (2010): 157–168.

Levite, A. *Offense and Defense in Israeli Military Doctrine*. Boulder, CO: Westview (1989).

Libicki, M. *Cyberdeterrence and Cyberwar*. Arlington, VA: Rand Corporation (2009).

Liff, A. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies*, 35, No. 3 (2012): 401–428.

Liles, S., Rogers, M., Dietz, J.E., and Larson, D. "Applying Traditional Military Principles to Cyber Warfare." In *Proceedings of the 4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski. Tallinn, Estonia: NATO CCD COE Publications (2012): 169–182.

Lin, H., and Zegart, A., eds. *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington: Brookings (2019).

Lin, H.S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law and Policy*, 4, No. 63 (2010): 63–86.

Lindsay, J.R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 22, No. 3 (2013): 365–404.
Lorents, P., and Ottis, R. "Knowledge Based Framework for Cyber Weapons and Conflict." Conference on Cyber Conflict Proceedings 2010. NATO CCD COE Tallinn, Estonia (2010): 129–142.
Loudermilk, M. "Iran Crisis Moves into Cyberspace." *Policy Watch*, 3151, Washington Institute for Near East Policy (July 9, 2019).
Lupovici, A. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives*, 17 (2016): 322–342.
Luttwak, E., and Yaniv, A. "Deterrence without the Bomb: The Politics of Israeli Strategy." *Naval War College Review*, 41, No. 4 (1988): 865–899.
Lynn, W. "The Pentagon's Cyberstrategy, One Year Later." *Foreign Affairs* (November 12, 2014). https://www.foreignaffairs.com/united-states/pentagons-cyberstrategy-one-year-later.
MacKenzie, D., and Wajcman, J. *The Social Shaping of Technology*. Buckingham, UK; Philadelphia: Open University Press (1999).
Mandiant. "M-Trends 2014: Beyond the Breach." *FireEye*, p. 9. https://www.mandiant.com/resources/mandiant-reports//
Maness, R., and Valeriano, B. "The Impact of Cyber Conflict on International Relations." *Armed Forces and Society*, 42, No. 2 (2015): 1–23.
Maoz, Z. *Defending the Holy Land: A Critical Analysis of Israel's Security and Foreign Policy*. Ann Arbor: University of Michigan Press (2006).
Matania, E. "Israel: The Making of a Cyber Power-Case Study." Issue Brief Five. Center for Cyber and Homeland Security. George Washington University. (September 2017).
Matania, E., and Paikowsky, D. "Influence Operations in Cyber: Characteristics and Insights." In *The Cognitive Campaign: Strategic and Intelligence Perspectives*, INSS Memorandum 197, ed. Y. Kuperwasser and D. Siman-Tov. (2019): 99–112. https://www.inss.org.il/publication/the-cognitive-campaign-strategic-and-intelligence-perspectives/.
Matania, E., and Rappaport, A. *Cybermania: How Israel Became a Global Force in the Realm That Is Shaping the Future of Humanity* (Hebrew). Israel: Kinneret, Zmora, Dvir (2021). (Also available in English.)
Matania, E., and Tal-Shir, E. "Continuous Terrain Remodelling: Gaining the Upper Hand in Cyber Defence." *Journal of Cyber Policy*, 5, No. 2 (2020): 285–301.
Matania, E., and Yoffe, L. "Some Things the Giant Could Learn from the Small: Unlearned Cyber Lessons for the US from Israel." *Cyber Defense Review*, 7, No. 1 (Winter 2022): 101–108.
Matania, E., Yoffe, L., and Goldstein, T. "Structuring the National Cyber Defense: In Evolution towards a Central Cyber Authority." *Journal of Cyber Policy*, 2, No. 1 (2017): 16–25.
Matania, E., Yoffe, L., and Mashkautsen, M. "A Three Layer Framework for a Comprehensive National Cyber-Security Strategy." *Georgetown Journal of International Affairs*, 27, No. 3 (2016): 77–84.
Matkowsky, J. "Israel's Attack on Hamas' Cyber Headquarters under Customary International Humanitarian Law." White Paper, SANS Institute (2019).
Maynard, T., and Beecroft, N. "Business Blackout." *Lloyd's Emerging Risk Report* (2015).
McGraw, G. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies*, 36, No. 1 (2013): 109–119.
McWhorter, D. "Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators." *FireEye Cybersecurity and Malware Protection* (February 19, 2013). https://www.mandiant.com/resources/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units.
Mearsheimer, J.J. *The Tragedy of Great Power Politics*. New York: Norton (2001).
Milevski, L. "Stuxtnet and Strategy: A Special Operation in Cyberspace." *JFQ*, 63 (2011): 64–69.
Miller, J.N., and Fontaine, R. "*A* New Era in US-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies are Reshaping Pathways to Crisis and Conflict." Belfer Center, Harvard Kennedy School, and CNAS (September 2017).

Mohurle, S., and Manishta Patil. "A Brief Study of WannaCry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science*, 8, No. 5 (2017): 1938–1940.

Moran, N. "A Cyber Early Warning Model." In *Inside Cyber Warfare*, ed. J. Carr. Cambridge, UK: O'Reilly (2012): 179–190.

Morgenthau, H.J. *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf (1948).

Mueller, M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press (2010).

Mueller, M., Grindal, K., Kuerbis, B., and Badiei, F. "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?" *The Cyber Defense Review*, 4, No. 1 (2019): 107–122.

Mueller, M., Schmidt, A., and Kuerbis, B. "Internet Security and Networked Governance in International Relations." *International Studies Review*, 15, No. 1 (2013): 86–104.

Nakasone, P.M., and Sulmeyer, M. "How to Compete in Cyberspace." *Foreign Affairs* (August 25, 2020). https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, DC: The National Academies Press (2010).

NATO Parliamentary Assembly, Science and Technology Committee. "NATO and the Cyber Age: Strengthening Security and Defense, Stabilizing Deterrence." NATO. (April 30, 2019).

Newsletter of the Ben Gurion University of the Negev. "BGU & You." Ben-Gurion University (Winter 2014).

Nissim, N, Yahalom, R., and Elovici, Y. "USB-based attacks." *Computers & Security*, 70 (2017): 675–688.

Nourian, A., and Madnick, S. "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet." *IEEE Transactions on Dependable and Secure Computing*, 15, No. 1 (January/February 2018).

Nuriel, N. "Cyber terrorism and Its Impact on the Civilian Sector." Herzliya Conference. (2011).

Nye, J. *Cyber Power*. Boston: Belfer Center (May 2010).

Nye, J. "Deterrence and Dissuasion in Cyberspace." *International Security*, 41, No. 3 (2016–2017): 44–71.

Nye J. *The Future of Power: Its Changing Nature and Use in the Twenty-First Century*. New York: Public Affairs. (2011).

O'Connell, M. "21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs." *Washington University Global Studies Law Review*, 13, No. 515 (2015): 515–533.

Office of the President. *Cyberspace Policy Review,* United States, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

OSCE. "Decision Number 1202: OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies, PC.DEC/1202." (March 10, 2016).

Pamment, J. "Can There Be a Deterrent Strategy for Influence Operations?" *Journal of Information Warfare*, 18, No. 3 (2019): 123–135.

Parmenter, R.C. "The Evolution of Preemptive Strikes in Israeli Operational Planning and Future Implications for Cyber Domain." School of Advanced Military Studies at the United States Army Command and General Staff College. (2013).

Peri, Y. *Generals in the Cabinet Room*. Washington, DC: US Institute of Peace (2006).

Perez, A.F. "Book Review: How I Learned to Stop Worrying and Love the Bots, and How I Learned to Start Worrying about Democracy Instead: A Review Essay on Striking Power: How Cyber, Robots, and Space Weapons Change the Rules of War." *Catholic University Journal of Law & Tech*, 27, No. 129 (2009): 129–143.

Perkovich, G., and Levite, A.E., eds. *Understanding Cyber Conflict: 14 Analogies*. Washington, DC: Georgetown University Press (2017).

Polin, B.A., and Ehrman, C.M. "The Curious Relationship between Military Service and Intrapreneurial Intentions in Israel." *Armed Forces and Society*, 46, No. 3 (2018): 438–453.

Pollitt, M. "Cyberterrorism—Fact or Fancy?" *Computer Fraud & Security*, 2 (1998): 8–10.

Radichel, T. "Case Study: Critical Controls that Could Have Prevented Target Breach." White Paper, SANS Institute InfoSec Reading Room (2014).

Raska, M. "Confronting Cyber Security Challenges: Israel's Evolving Cyber Defense Strategy." Policy Report, Rajaratnam School of International Studies (2015).

Rattray, G., and Healey, J. "Non-State Actors and Cyber Conflict." In *America's Cyber Future: Security and Prosperity in the Information Age*, ed. K.M. Lord, M. McConnell, P. Schwartz, R. Fontaine, T. Sharp, and W. Rogers. Center for a New American Security (June 2011). https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238&focal=none.

Razin, A. *Israel and the World Economy*. Cambridge, MA: MIT Press (2018).

Richet, J. *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*. Hershey, Pennsylvania: Information Science Reference, an imprint of IGI Global (2015).

Rid, T. *Cyber War Will Not Take Place*. London: C. Hurst and Co (2013).

Rid, T., and Buchanan, B. "Attributing Cyber Attacks." *The Journal of Strategic Studies*, 38, No. 1–2 (2015): 4–37.

Rid, T., and McBurney, P. "Cyber Weapons." *The RUSI Journal*, 157 (2012): 6–13.

Rodman, D. *Sword Shield of Zion: The Israel Air Force and the Arab-Israeli Conflict, 1948–2012*. Brighton, UK: Sussex Academic Press (2013).

Rosenbach, E., Kayyem, J., and Mitra, L. "The Limits of Cyber Offense: Why America Struggles to Fight Back." *Foreign Affairs* (August 11, 2021). https://www.foreignaffairs.com/articles/united-states/2021-08-11/limits-cyberoffense.

Rosenberg, S., and Israel Defense Forces. *Deterring Terror: How Israel Confronts the Next Generation of Threats*. English Translation of the Official Strategy of the Israel Defense Forces. Belfer Center Special Report (2016).

Rosenberger, L., "Making Cyberspace Safe for Democracy." *Foreign Affairs* (2020). https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Rosner, Y. and Siman-Tov, D. "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion." *INSS Insight*, 1031 (March 8, 2018). https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/.

Rovner, J. "Cyber War as an Intelligence Contest." *War on the Rocks* (September 16, 2019).

Rubin, U. "'Iron Dome' vs. Grad Rockets: A Dress Rehearsal for an All-Out War?" Perspectives Papers 173, BESA (July 3, 2012).

Rubin, U. "The Rocket Campaign against Israel during the 2006 Lebanon War." Mideast Security and Policy Studies 71, BESA (June 2007).

Russell, A. *Strategic A2/AD in Cyberspace*. Cambridge: Cambridge University Press (2017).

Sanger, D.E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House (2012 and 2013).

Sanger, D.E. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Crown (2018).

Saressalo, T.J. "Israeli Defense Forces' Information Operations 2006–2014." *Journal of Information Warfare*, 18, No. 1, Parts 1–3 (2019): 87–126.

Saydjari, O. "Cyber Defense: Art to Science." *Communications of the ACM*, 47, No. 3 (2014): 52–57.

Saydjari, O.S. "Cyber Defense: Art to Science." *Communications of the Association for Computing Machinery*, 47, No. 3 (2004): 52–57.

Schaake, M. "The Lawless Realm: Countering the Real Cyber Threat." *Foreign Affairs* (November/December 2020): 27–33.

Scharre, A., and Riikonen, A. "Defense Technology Strategy," *Center for a New American Security* (2020): 1–18. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Defense-Technology-Strategy-2.pdf?mtime=20201116164927&focal=none.

Schmidt, E., and Cohen, J. *The New Digital Age: Transforming Nations, Business, and Our Lives*. New York: Vintage Books (2014).

Schmitt, M. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal Online*, 54 (2012): 13–37.

Schmitt, M. "Israel's Cautious Perspective on International Law in Cyberspace." *Blog of the European Journal of International Law*, Parts 1 and 2 (December 17, 2020). https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/.

Schmitt, M., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York: Cambridge University Press (2013).

Schmitt, M., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York: Cambridge University Press (2017).

Schmitt, M. "Top Expert Backgrounder: Russia's SolarWinds Operation and International Law." *Just Security* (December 21, 2020). https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

Schneier, B. "Eight Ways to Stay Ahead of Influence Operations." *Foreign Policy* (August 12, 2019). https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

Schöndorf, R. "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *Blog of the European Journal of International Law* (December 9, 2020).

Schwab, K. "The Global Competitiveness Report." World Economic Forum (2016).

Schweitzer, Y., Siboni, G., and Yogev, E. "Cyberspace and Terrorist Organizations." *Military and Strategic Affairs*, 5, No. 3 (2013): 17–26.

Segal, A. *The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Ages*. New York: Public Affairs (2017).

Senor, S., and Singer, S. *Start Up Nation*. New York: Hachette Book Group (2009).

Shabtai, S. "Recommendation for the National Center for Cyber Defense: Recognize the Limitations of Regulation." Perspectives #444, BESA Center, Ramat Gan (April 6, 2017).

Shakarian, P., Shakarian, J., and Ruef, A. *Elsevier's Introduction to Cyber-Warfare*. 1st Edition. Boston, MA: Elsevier (June 14, 2013).

Shamir, E., and Hecht, E. "Gaza 2014: Israel's Attrition vs. Hamas' Exhaustion." *Parameters*, 44, No. 4 (2014–2015): 81–90.

Shamir, R., and Bachar, E. "Defending Israel Selections from Cyber Attack—What Should Be Done? (Hebrew)." Israel Democracy Institute, Policy Study 136 (January 2019).

Shelah, O. *HaOmetz Lenatzeach: The Courage to Win.* Tel Aviv: Yediot Books (2015).

Shelah, O. *The Israeli Army: A Radical Proposal* (Hebrew). Or Yehuda, Israel: Kinneret Zmora-Bitan (2003).

Sheniak, A. "Development of the State in the Online Frontier Realm: A Theoretical and Historical Comparison (Hebrew)." *Maarachot*, 3 (December 2014): 13–44.

Shkedi, D. "The Cybersecurity Sector in Israel (Report)." Embassy of India (2015).

Shuker, P., and Siboni, G. "The Threat of Foreign Interference in the 2019 Elections in Israel and Ways of Handling It." *Cyber, Intelligence and Security*, 3, No. 1 (2019): 27–40.

Siboni, G, ed. *Cyberspace and National Authority—Selected Articles*. Institute for National Security Studies (2013).

Siboni, G. "Protecting Critical Assets and Infrastructures from Cyber Attacks." In *Cyberspace and National Security—Selected Articles*, ed. G. Siboni. Institute for National Security Studies (2013): 93–101.

Siboni, G. "The First Cognitive War." Strategic Survey for Israel 2016–2017, *Institute for National Security Studies* (2016): 215–223. https://www.inss.org.il/wp-content/uploads/systemfiles/The%20Impact%20of%20Cyberspace%20on%20Asymmetric%20Conflict%20in%20the%20Middle%20East%20-%20An%20article%20by%20Gabi%20Siboni%20in%20Georgetown%20Journal%20of%20International%20Affairs.pdf.

Siboni, G. "The Impact of Cyberspace on Asymmetric Conflict in the Middle East." *Georgetown Journal for International Affairs* (April 28, 2015). https://www.inss.org.il/wp-content/

uploads/systemfiles/The%20Impact%20of%20Cyberspace%20on%20Asymmetric%20Conflict%20in%20the%20Middle%20East%20-%20An%20article%20by%20Gabi%20Siboni%20in%20Georgetown%20Journal%20of%20International%20Affairs.pdf.

Siboni, G., Abramski, L., and Sapir, G. "Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy." *Cyber, Intelligence and Security*, 4, No. 1 (2020): 21–40.

Siboni, G., and Assaf, O. "Guidelines for a National Cyber Strategy." Memorandum 153, Institute for National Security Studies (2016).

Siboni, G., Cohen, D., and Rotbart, A. "The Threat of Terrorist Organizations in Cyberspace." *Military and Strategic Affairs*, 5, No. 3 (2013): 3–29.

Siboni, G., and Klein, H. "Guidelines for the Management of Cyber Risk." *Cyber, Intelligence, and Security*, 2, No. 2 (2018): 23–38.

Siboni, G., and Kronenfield, S. "The Iranian Cyber Offensive During Operation Protective Edge." Institute for National Security Studies (August 26, 2014).

Siboni, G., and Kronenfeld, S. "Iran and Cyberspace Warfare." In *Cyberspace and National Security—Selected Articles*, ed. Gabi Siboni. Institute for National Security Studies (2013): 81–103.

Siboni, G., and Sivan-Sevilla, I. "Israeli Cyberspace Regulation: A Conceptual Framework, Inherent Challenges, and Normative Recommendations." *Cyber, Intelligence, and Security*, 1, No. 1 (2017): 83–102.

Siboni, G., and Sivan-Sevilla, I. "Regulation in Cyberspace." Memorandum 190, Institute for National Security Studies (2019).

Silber, J. "Cyber Vandalism—Not Warfare." *Ynetnews.com* (January 26, 2012). http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

Siman-Tov, D., and Even, S. "A New Level in the Cyber War between Israel and Iran." *INSS Insight* 1328 (June 3, 2020). https://www.jstor.org/stable/resrep25542#metadata_info_tab_contents.

Siman-Tov, D., and Even, S. "Cyber Warfare: Concepts and Strategic Trends." Memorandum No. 117, Institute for National Security Studies (2012).

Singer, S., and Friedman, A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press (2014).

Siniver, A. "Israeli Identities and the Politics of Thread: A Constructivist Interpretation." *Ethnopolitics*, 11, No. 1 (2012): 24–42.

Sklerov, M.J. "The United States Should Use Active Defenses to Defend Its Critical Information Systems." In *Inside Cyber Warfare*, ed. J. Carr, Cambridge, UK: O'Reilly (2012): 194–196.

Slayton, R. "What Is the Cyber Offense-Defense Balance? Concepts, Causes, and Assessment." *International Security*, 41, No. 3 (2016/2017): 72–109.

Smeets, M. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies*, 41, No. 1–2 (2017): 6–32.

Sobelman, D. "Learning to Deter: Deterrence Failure and Success in the Israel-Hezbollah Conflict, 2006–2016." *International Security*, 41, No. 3 (Winter 2016/2017): 151–196.

Sofaer, A.D., Clark, D., and Diffie, W. "Cyber Security and International Agreements." In *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy*. National Research Council. Washington, DC: The National Academies Press (2010): 179–206, http://www.nap.edu/catalog/12997.html.

Steinherz, T. "Israeli Innovation in Cyber-Technology." Herzlia Conference. (June 9, 2014).

Stockburger, P.Z. "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum." *American University International Law Review*, 31, No. 4 (2016): 545–592.

Straub, J. "Mutual Assured Destruction in Information, Influence and Cyber Warfare: Comparing, Contrasting and Combining Relevant Scenarios." *Technology in Society*, 59 (2019): 1–9.

Stott, P. "Iranian Influence Networks in the United Kingdom: Audit and Analysis." Henry Jackson Society (June 2021).

Sulmeyer, M. *Cyberspace: A Growing Domain for Iranian Disruption*. Washington DC: Center for Strategic and International Studies (2017).

Sulmeyer, M. "How the US Can Play Cyber Defense: Deterrence Isn't Enough." *Foreign Affairs* (March 22, 2018). https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

Swed, O., and Butler, J.S. "Military Capital in the Israeli Hi-Tech Industry." *Armed Forces in Society*, 41, No. 1 (2013): 123–141.

Tabansky, L. "Critical Infrastructure Protection against Cyber Threats." In *Cyberspace and National Security—Selected Articles*, ed. Siboni, G. Institute for National Security Studies (2013): 61–78.

Tabansky, L. "Cyber Power in the Changing Middle East." *Turkish Policy Quarterly*, 15, No. 1 (2016): 107–114.

Tabansky, L. "Cybercrime: A National Security Issue?" *Military and Strategic Affairs*, Institute for National Security Studies, 4, No. 3 (2012): 117–136.

Tabansky, L. "Israel Defense Forces and National Cyber Defense." *Connections: The Quarterly Journal*, 19, No. 1 (2020): 45–62.

Tabansky, L., and Ben-Israel, I. *Cyber Security in Israel*. New York: Springer (2015).

Tabatabai, A.M. "Iran's Authoritarian Playbook: The Tactics, Doctrine and Objectives behind Iran's Influence Operations." Alliance for Securing Democracy (2020).

Tal, I. *National Security: The Few against the Many* (Hebrew). Tel Aviv: Dvir (1996).

Tamir, D. "Israeli Cyber Defense Needs a National Cyber System." MirYam Institute (June 1, 2021).

Taylor, M.Z. *The Politics of Innovation: Why Some Countries Are Better Than Others at Science and Technology*. New York: Oxford University Press (2016).

The India Conference on Cyber Security and Cyber Governance. "International Public Private Partnership in Cyber Governance (Panel)." Observer Research Foundation and Digital Economy Committee (October 14–15, 2013): 33–35.

Tira, R. "Developing a Doctrine for Cyber Warfare in the Conventional Campaign." *Cyber, Intelligence and Security*, 2, No. 1 (2018): 93–104.

Tor, U. "Cumulative Deterrence as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies*, 40, No. 1–2 (2015): 92–117.

Trobisch, J. *Challenges in the Protection of US Critical Infrastructure in the Cyber Realm*. United States Army Command and General Staff College. School of Advanced Military Studies (2014).

Unal, B. "Cybersecurity of NATO's Space-Based Strategic Assets." *Royal Institute of International Affairs* (2019). https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets.

United Against a Nuclear Iran (UANI). "The Iranian Cyber Threat." *UANI* (May 2022). https://www.unitedagainstnuclearіran.com/sites/default/files/UPDATE%20-%20The%20Iranian%20Cyber%20Threat_9.7.22_JC_JMB_CMJ.pdf.

United Nations. *Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security* (2015).

United Nations. *Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security* (2021).

University of California Office of the President. "The University of California and Israel's Innovation Authority Sign Cooperation Agreement." (February 17, 2017).

Valeriano, B., Jensen, B.M., and Maness, R. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press (2018).

Valeriano, B., and Maness, R. *Cyber War versus Cyber Realities*. New York: Oxford University Press (2015).

Valeriano, B., and Maness, R. "Persistent Enemies and Cyberwar." In *Cyberspace and National Security*, ed. Derek S. Reveron. Washington DC: Georgetown University Press (2012): 139–157.

Walt, S. "The Enduring Relevance of the Realist Tradition." In *Political Science: State of the Discipline III*, ed. I. Katznelson and H. Milner. New York: W.W. Norton and Co. (2002): 197–209.

Waltz, K.N. *Man, the State, and War*. New York: Columbia University Press (1954).

Waltz, K.N. *Theory of International Politics*. New York: McGraw-Hill (1979).
Wang, H., Lau, N., and Gerdes, R.M. "Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures through Work Domain Analysis." *Human Factors*, 60, No. 5 (August 2018): 699–718.
Wechsler, O. "Germany's Cyber Strategy, Government and Military Preparations for Facing Cyber Threats, Cyber." *Intelligence and Security*, 2, No. 1 (2018): 55–72.
Weimann, G. "Cyberterrorism: How Real Is the Threat?" *Special Report for the United States Institute of Peace* 119 (December 2004): 1–12.
Weimann, G. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism*, 28, No. 2 (2005): 129–149.
Weinmann, G. "How Modern Terrorism Uses the Internet." *Special Report 116 for the United States Institute for Peace* (March 2004): 1–12.
Weinmann, G. *Terror on the Internet*. Washington, DC: United States Institute of Peace Press (2006).
Wendt, A. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization*, 36, No. 2 (1992): 391–425.
Wendt, A. *Social Theory of International Politics*. Cambridge, UK: Cambridge University Press (1999).
Williams, R., and Edge, D. "The Social Shaping of Technology." *Research Policy*, 25, No. 6 (1996): 865–899.
Yaniv, A. *Deterrence without the Bomb: The Politics of Israeli Strategy*. Lexington, MA: D.C. Heath and Company (1987).
Yaniv, A., ed. *National Security and Democracy in Israel*. Boulder, CO: Lynne Reiner (1993).
Yariv, A. "Strategic Depth." *Jerusalem Quarterly*, 17 (1980): 3–12.
Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown (2014).
Zetter, K., and Modderkolk, H. "How a Secret Dutch Mole Aided the US-Israeli Stuxnet Cyber Attack on Iran." Yahoo.com (September 2, 2019)
Zippori, M. "Hackers Attack Two Israeli Websites." *CNN* (January 26, 2012). http://www.cnn.com/2012/01/16/world/meast/israel-hacking-attack/.
Zittrain, J. *The Future of the Internet—And How to Stop It*. London: Yale University Press & Penguin UK (2008).
Zrahia, A. "A Multidisciplinary Analysis of Cyber Information Sharing." *Military and Strategic Affairs*, 6, No. 3 (2014): 59–77.

INDEX

For the benefit of digital users, indexed terms that span two pages (e.g., 52–53) may, on occasion, appear on only one of those pages.