CENTER for STRATEGIC LEADERSHIP

CSL

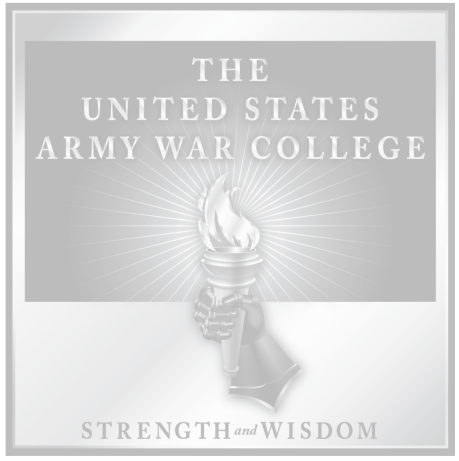
U.S. ARMY WAR COLLEGE

# RETHINKING SOVEREIGNTY IN THE CONEXT OF CYBERSPACE

## THE CYBER SOVEREIGNTY WORKSHOP SERIES

Written and Compiled by
Cynthia E. Ayers

# RETHINKING SOVEREIGNTY IN THE CONTEXT OF CYBERSPACE


THE
UNITED STATES
ARMY WAR COLLEGE
STRENGTH and WISDOM

# RETHINKING SOVEREIGNTY IN THE CONTEXT OF CYBERSPACE

## The Cyber Sovereignty Workshop Series

**Written and Compiled by**
**Cynthia E. Ayers**

# Acknowledgements

This report documents the proceedings of a series of three Cyber Sovereignty Workshops, conducted February 10-12, 2015; June 23-25, 2015; and June 7-9, 2016 by the Mission Command and Cyber Division, Center for Strategic Leadership, United States Army War College, in partnership with United States Cyber Command and United States Army Cyber Command.

Editors:

Dr. Jeffrey L. Groh
Colonel (Ret.) James C. Markley
Colonel Charles E. Grindle, Ph.D.
Mr. Anthony Allard

2015 Workshop Coordinators:

Professor William O. Waddell
Brigadier General (Ret.) Kenneth D. Chrosniak
Ms. Cynthia E. Ayers

2016 Workshop Coordinators:

Colonel James A. Skelton
Mr. Benjamin C. Leitzel
Ms. Cynthia E. Ayers
Mr. Anthony Allard
Mr. Al Epperson

Rapporteurs:

February 2015 Workshop

Dr. Jeffrey L. Groh
Colonel (Ret.) James C. Markley
Colonel Charles E. Grindle, Ph.D.

June 2015 Workshop
Professor James O. Kievit
Colonel (Ret.) James C. Markley
Colonel Stephanie Howard

June 2016 Workshop
Mr. Robert Chicci
Major Robert Page

Drilling Individual Mobilization Augmentees

February 2015 Workshop
Colonel Brian Adelson
Colonel Damon Igou
Sergeant First Class Richard Phelps

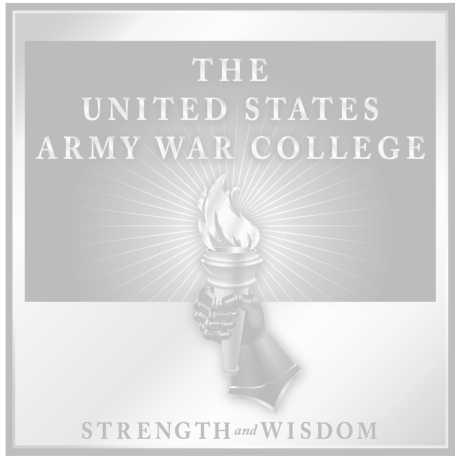
June 2015 Workshop
Lieutenant Colonel Wayne Grant
Lieutenant Colonel Jae Song
Lieutenant Colonel Paul Matura
Sergeant First Class (P) Richard Phelps



**This publication is available on line at:**

**http://www.csl.army.mil/AllPublications.aspx**

**U.S. ARMY WAR COLLEGE**
**CARLISLE BARRACKS, PENNSYLVANIA 17013**
**December 2016**


THE
UNITED STATES
ARMY WAR COLLEGE
STRENGTH and WISDOM

# Contents

# Introduction

Sovereignty in cyberspace has become a recent topic of concern. From the perspective of some malicious cyber actors, the Westphalian form of sovereignty can be considered completely irrelevant; yet it remains an important concept upon which policy, laws, regulations, conventions and treaties are built, and thus is the basis for the determination of policy and strategy in Western nations – especially in regard to U.S. response.

Does the concept of sovereignty apply to cyberspace? Is the maintenance of territorial and conceptual boundaries associated with national sovereignty compatible with an interconnected, independent cyberspace? If not, is the default alternative a reinterpretation of the power and authority of nation-states? Must reconstruction or deconstruction of politically sovereign entities occur in order to conform to the inherently "free" nature of a digital era?

Adoption of technological innovation is occurring across the globe with astounding rapidity. Yet consideration of the ramifications of a highly-wired world to traditional jurisdictions and national autonomy has not kept pace. The wide disbursement of web infrastructure, in conjunction with attempts by a variety of aggressors to use the Internet for control and "power projection," now "challenge traditional ideas of security, stability, and sovereignty."[1]

Cyberspace is both essential to the existence of governments and those governed, and dangerous in its relative anonymity and connectivity to virtually all corners of the world. It is a place for economics and civil discourse while simultaneously a battleground for war waged by nation-states, adversarial groups and autonomous actors. In war, not all participants play by the same rules. Regulations developed for reasons of adhering to ethical norms and cultural traditions tend to slow response and, even with the best defense, give attackers who lack similar restrictions the distinct – and crucial – advantage of time. Time, in cyberspace, can be measured in nanoseconds.

Testimony before a House Armed Services Subcommittee by incoming USCYBERCOM Commander Admiral Michael Rogers, revealed that U.S. cyber forces "have had the equivalent of a close-in fight with an adversary, which taught us how to maneuver and gain the initiative that means the difference between victory and defeat." Still, he conceded: "Neither the U.S. Government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help."[2] As to exactly what that "help" could be remains in question.

While the private sector might be of assistance in the cyber defense realm, their active resistance in the form of counterattack is, to this point, illegal.[3] For those living and working within the sovereign geographical boundaries of the United States, cyber response (a.k.a. retaliation) is a highly debated and regulated option reserved for federal entities authorized to defend the nation against adversaries operating in cyberspace. Due to the very nature of cyber threat, however, both civilian and military equities are targets. Statistics reveal that attacks are increasing in quantity and sophistication for both sectors.[4]

A variety of legal, regulatory, and accepted self-limiting obstacles are in place, hindering public/private cooperation in cyber defense and counterattack. Reconstructing laws and regulations to make them more beneficial to those who are "victimized" by attacks, as well as to those who must guide and guard national security is a slow and arduous process. There is ongoing debate regarding the applicability of traditional ethics and laws to cyberwarfare.[5] The fact that cyberspace functionality and capabilities are still largely enigmatic to elected leaders (with elucidation unlikely due to the pace of technological change) compounds the problem of coming to a consensus. Simply put, the conventional approach to policy-making in the United States is so deliberative, and so dependent on historical context that it might actually be incompatible with the establishment of viable cyber statutes.[6] Furthermore, political quiescence inhibits domestic and international agreements regarding cyber strategy and doctrine.

Currently, national cyber protection relies on mitigation using passive defense (e.g. information assurance, cybersecurity, and defense-in-depth); yet reliance on a blanket of protection is "unsustainable."[7]

Retaliation, or "response-in-kind," appears to be lacking (with few exceptions), mainly because of difficulties in determining attribution to the source of cyberattacks, system infiltration, data manipulation, and malware.[8] The time lag invariably associated with post-event (or post recognition) analysis can make meaningful response awkward or impossible. Also, vague, confusing, and in some cases, non-existent policies and strategies (as previously mentioned), tend to retard the operational decision-making process.

Cybersecurity is, and will continue to be, both costly and crucial. Concerns are rising within private industry and all levels of government about their ability to keep pace with attackers and infiltrators using cybersecurity methods alone.[9] Are measures consisting only of passive defense sufficient? Is passive defense the only kind of defense that conforms to U.S. ethical and moral standards? If active response can be justified, what would that response entail, and who should it come from?

Past anxieties have centered on the potential for privately initiated acts, or unauthorized actions of "rogue operators" in cyberspace to spark a larger cyberwar,[10] but the provocations of nation-states utilizing proxies presents a much bigger problem for both public and private sectors.[11] If multiple and diverse (public and private) avenues of response are eventually authorized, what would the implications be? Would a spontaneous, multilateral counterattack have an adverse or advantageous effect on the security of the nation?

National defense options ultimately depend on attribution and timely response, and cyber attackers can be emboldened by a minimal or non-existent counterstrike.[12] Escalation by nefarious actors (whether for the purpose of probing, surveillance, espionage, infiltration, or attack) is now the norm, as evidenced by statistics reported by business and industry. "Attackers are moving faster, defenses are not."[13]

Cyber attackers are rarely (if ever) deterred by law, nor do they necessarily adhere to "just war" conventions. Federal officials at the cabinet level,[14] as well as a large number of business executives[15] are worried about the consequences of major malicious cyber events, to include targeting of critical infrastructure control systems. They warn that a "first strike" option can be devastating, whether the target is a

government organization or a business; and response (legal, ethical, or otherwise) may ultimately not be possible. In what has been described as a "Cyber Pearl Harbor,"[16] a serious effort perpetrated as a first strike maneuver "could paralyze the nation and create a profound new sense of vulnerability."[17]

Former Chairman, Joint Chiefs of Staff Admiral Mike Mullen named cyberattacks as one of two "existential" threats to the United States – the other being nuclear weapons. He noted: "we're a long way from" establishing the kind of doctrine developed for strategic nuclear weapons and warfare during the cold war.[18] Yet China and Russia have taken bold steps toward cooperative policy and strategy development in cyberspace, even to the point of proposing partnerships in the formation and preservation of cyber sovereignty.[19]

Recent successful "hacks," allegedly carried out by professionals acting on behalf of, or in concert with nation-states (e.g. against Sony,[20] the Office of Personnel Management [OPM][21] and the Internal Revenue Service [IRS]),[22] have heightened concerns about cyber warfare and sovereignty in the context of cyberspace. To maintain the integrity of U.S. and allied sovereign borders, it is imperative that security measures and defenses are coordinated and choreographed at the policy, strategy, and operational levels in the cyber domain, as well as in the physical world.

In consideration of this imperative, the Mission Command and Cyber Division, Center for Strategic Leadership, United States Army War College, in partnership with United States Cyber Command (USCYBERCOM) and United States Army Cyber Command (ARCYBER), planned and conducted a series of workshops focused on sovereignty in cyberspace. The intent of these workshops, and of this report, is to bring clarity to questions regarding sovereignty in the cyberspace domain (including many of those listed above) to the extent possible within the limitations of an unclassified workshop format.

## Purpose

The purpose of this series of mission critical workshops was to consider the concept of sovereignty in cyberspace, given three areas of focus: Policy, Strategy, and Theory/Operations. These workshops provided an

unclassified forum for cross-sector discussions about actions planned and taken, policies and strategies under consideration, and decisions made concerning security and defense of the nation (public and private sectors) within the cyberspace domain.

It is crucial that military and civilian leaders understand the national and international aspects of sovereignty issues in cyberspace. The determination of what constitutes cyber sovereignty will greatly influence identification and understanding of threats, Department of Defense (DoD) preparation of the battlefield, the development of capabilities, the identification of participants, and planning for cyberspace operations. Considering the stakes, U.S. leaders cannot afford the consequences of allowing the enemy to define the boundaries of cyber sovereignty and the rules of cyberspace engagement.

## Methodology

The general concept for the three workshops consisted of in-depth discussions held mostly within breakout groups over a three-day period, interspersed with plenary presentations delivered by subject matter experts (SMEs), and followed by outbriefs consisting of problems considered, solutions explored, and proposals developed by each group. An exception was made for the third workshop in the series, where plenary presentations and discussion sessions (with participation by all attendees), occurred within the same room.*


Attendees participated on a non-attribution basis, with the exception of content authorized by keynote and plenary speakers (see Appendix

* The decision to use one group discussion, as opposed to breakout groups, was largely due to limited attendance driven by recent DoD regulations.

A). This workshop report is a synthesis of contributions from speaker presentations, and group deliberations merged with a review of pertinent literature for substantiation of the relevant and critical nature of topics raised.

Each workshop was held at an unclassified level in order to encourage private sector involvement, as well as to ensure that published results can be readily accessed and acted upon by civilian cyber strategists (private and public sector); policy makers at the federal, state and local levels; and DoD senior leadership. All participants received briefings on options and recommendations for the way forward at the end of each workshop.

Workshop invitees throughout the series included representatives of the following groups/organizations:

- DoD/Military (USAWC, USCYBERCOM, ARCYBER, Navy, Army Cyber Institute, others)
- Department of Homeland Security (DHS)
- Department of Justice (DOJ)
- Legal Professionals, Government and Private
- Academia
- Private Industry
- Army "Fellows"
- Think Tanks

# Chapter 1: Policy

## General Overview

The potential for cyberattacks against the United States was the number one global threat listed within the 2013,[1] 2014,[2] 2015,[3] and 2016[4] Worldwide Threat Assessments conveyed annually to Congress by the Director of National Intelligence (DNI). The DNI's 2013 assessment followed a year of warnings by cabinet-level officials about plausible, devastatingly effective adversarial cyber events.[5] For additional emphasis, a Presidential Policy Directive (PPD-21)[6] and an Executive Order (EO 13636),[7] both on cybersecurity and critical Infrastructure, immediately preceded the DNI's 2013 testimony to Congress.

Considering the possibility of "return-fire" from Iran after a *New York Times* article claimed that the United States was responsible for release of the Stuxnet virus against Iranian nuclear control systems,[8] the intensity of attention given to cyber threat should not have been surprising. Yet, publicity accompanying the warnings and Executive actions may have had a dual purpose. Prompting public awareness of a possible cyber strike against the United States would be the most obvious reason. Prodding policy-makers for passage of serious, meaningful cyber legislation may have been another. The public may now be more aware; but cyber legislation continues to be deficient.

More than two years after the *New York Times* Stuxnet revelation, Jessica Herrera-Flannigan, former Senior Counsel at the DOJ's Computer Crime and Intellectual Property Section, opined that policy, as it currently exists in the realm of national cybersecurity, is "still stuck in the '90s." Ms. Herrera decried that in spite of almost two decades of "countless reports, think-tank events, congressional hearings, legislation and administration action," cyber policy discourse has not advanced past the initial focus on the need for "shared responsibilities, incentives, R&D investment, government procurement, information sharing, insurance and standards."[9]

On February 10-12, 2015 – only a few months after the publication of Ms. Herrera's critique – a group of subject matter experts met at the Center for Strategic Leadership, U.S. Army War College for the first in a series of three workshops dealing with the fundamental issue of sovereignty in the context of cyberspace. The focus of the first workshop was specifically on the policy arena, with the goal of identifying gaps and offering recommendations to policy-makers and senior leaders. The intention was to "move the ball forward" with regard to cyberspace legislation.

**Objectives**

The Policy workshop had three major objectives:

- Develop/propose definitions of key terms and concepts (for those that remain in flux);
- Secure a relevant understanding of and consensus on existing gaps in national policy, and establish how/who best to respond to them with coordinated and effective proposals; and
- Offer recommendations to policy-makers and senior leaders addressing identified challenges and issues.

**Research**

Participants examined relevant documentation for topic applicability and adequacy with regard to current and future needs, including:

- Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity* (12 Feb 2013);[10]
- House Resolution (H.R.) 624 (pending), *Cyber Intelligence Sharing and Protection Act (April 22, 2013)*;[11]
- H.R. 3696 (pending), *The National Cybersecurity and Critical Infrastructure Protection Act (2013-2014)*;[12]
- The National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014);[13] and
- *The Department of Defense Strategy for Operating in Cyberspace* (July 14, 2011).[14]

Research questions seen as key to identifying critical cyber policy needs were:

- What are the gaps and vulnerabilities caused by or resulting from a lack of substantive, comprehensive cyber policy?
- What responsibilities do specific government agencies have in the cyber sovereignty and policy arenas?
- When do cyber threats shift from a matter of national security to that of national defense?
- How do we address cyber policy-induced national defense and security vulnerabilities?
- What policy response is appropriate to the international and domestic pressures that exacerbate critical vulnerabilities and affect our ability to maintain cyber sovereignty?

Breakout groups for this workshop concentrated specifically on:

- International considerations
- Defense Support of Civil Authorities (DSCA) options
- DoD concerns and requirements

Participants considered the research questions within the context of the current environment. In order to address identified challenges, group representatives captured recommendations that might advance, change, or otherwise enhance cyber-related policy.

**Definitions**

One obstacle to progress in the policy arena is the lack of a standardized cyberspace lexicon. Although the DoD is working to resolve conflicting definitions, constant revisions and security classifications are an enduring dilemma for those who must adhere to specific guidelines – especially in a legal sense. This is not a new problem – those involved in counterterrorism efforts may sympathize with the conundrum as the debate over definitions, as well as terms of use before and after the attacks of 9/11 continue to challenge analysts and reporters. Thus, extensive discussion centered on definitions of key terms and concepts.

Concerns included a lack of specific, standardized definitions for use "across-the-board." Differences continue to "muddy the waters" when

reporting is mixed (e.g. private/public). Certain words and phrases reserved for cyberspace (such as "cyberattack") have specific legal meanings when used by government entities, which establish levels and types of response as well as responsibilities and authorities to act. Private sector representatives and members of mass media often use the same wording without regard to legalities or implications. This lack of baseline verbiage for one-and-all creates confusion between public and private sectors, while raising false expectations in the public-at-large.

Ultimately, with only a few exceptions (specifically those subject to legal requirements for use such as "cyberattack," "cyber use of force," and "cyber act of war" as well as the concept of "cyber sovereignty"), most definitions delineated in Joint Publications 1-02, 3-12 (R) and version 5.7 of the USCYBERCOM Cyber Lexicon sufficed for the purposes of this workshop. Differences remain as to whether there is appropriate clarity between cyberspace security and cyberspace defense. In addition, attempts to create a standard definition of "cyber sovereignty" resulted in stalemate; but the final consensus was that there was no need – that the question inherent to workshop proceedings actually referred to the maintenance of national sovereignty in consideration of a more fluid, flexible cyberspace reality.

One breakout group engaged in debate over the definition of cyberspace noting:

> *"The definition…makes clear the 'physical' aspects such as the infrastructure. However, since cyberspace is not a static entity, this definition falls short. Cyberspace is indeed a network of IT infrastructures but it is also a medium by which various forms of human communication are enabled. As such, the logical and cyber persona aspects of cyberspace could in some way be added to the current definition."*[15]

Indeed, sovereignty in cyberspace is dependent to a large degree on these "non-IT" aspects.

**Gaps and Vulnerabilities**

What are the gaps and vulnerabilities caused by or resulting from a lack of substantive, comprehensive cyber policy? Are there ways to address them that might be acceptable to all relevant parties?

One notable vulnerability is a lack of situational awareness by those targeted, often caused by classification (in the public sector) and risk management (in the private sector). Depending on the organization(s) performing analysis on cyberattacks, data derived from the process – and indeed, the entire event – may be classified or labeled "close hold". Conventional intelligence community wisdom dictates the maintenance of tight security when/if the release of intelligence data has the potential to threaten national security interests. Given these restrictions, private organizations may not fully comprehend current threat levels or have sufficient data to address specific attacks. Alternatively, private sector groups may not find it economically advisable to confess data breaches (essentially conceding vulnerability and risking public disclosure), regardless of regulatory "encouragement."

Workshop participants noted that the lack of a long-term interagency cyberspace campaign plan (for deterrence, detection, defense, protection, and response) hinders progress in all areas of cybersecurity and defense. They further highlighted the fact that there is no specific organization designated to deter and defend against cyberspace threats to critical infrastructure, and that there is no realistic government capacity to provide defensive countermeasures extending to the private sector.

Elements of critical infrastructure that are classified "dual use"[16] (e.g. critical to government/military and civilian existence) are already under constant threat from cyber intrusion and attacks by state and non-state actors. Executive actions (EO 13636 – *Improving Critical Infrastructure Cybersecurity* and PPD-21 –*Critical Infrastructure Security and Resilience* )[17] and pending policy (H.R. 3696 – *National Cybersecurity and Critical Infrastructure Protection Act of 2014*)[18] outlining security and defense of critical infrastructure have been vague enough to allow for avoidance of responsibility, and were determined by attendees to be insufficient for comprehensive, service-specific, doctrinal development.

Division of effort in the realm of critical infrastructure protection is highly complex, with many stakeholders weighing into the mix. Increasing numbers and sophistication of cyberattacks have resulted in several efforts to address the problem, but not without criticism. For instance, an unprecedented agreement between DHS and DoD to "align their capabilities to bolster defenses against cyber-attack" in

2010[19] raised the specter of a breach of mandated separation of external and domestic missions, mostly by organizations affiliated with the intelligence community.[20]

EO 13636, designed to provide a means to enhance cybersecurity through "partnership with the owners and operators of critical infrastructure" using a "risk-based approach," followed in 2013.[21] Within the context of E.O. 13636, however, information sharing remained voluntary and limited to "eligible" service providers. While it codified the participation of intelligence agencies with missions specific to external threat, E.O 13636 sought to overcome criticism by addressing privacy concerns and protection of civil liberties.[22] Because it lacked "teeth" and essentially echoed a cry for intelligence sharing that has been ongoing since the terrorist attacks of 9/11, participants deemed E.O. 13636 insufficient to satisfy the need for clarity in mission delineations and responsibilities.

In January 2015 (immediately prior to workshop proceedings), the President signed another Executive Order (EO 13687[23]) in response to a series of cyberattacks attributed to the government of North Korea, collectively dubbed the "Sony Pictures Hack." [24] This EO authorized additional sanctions on North Korea to be imposed by the Secretary of the Treasury, and was written in much the same manner as EO 13466 *Continuing Certain Restrictions With Respect to North Korea and North Korean Nationals* (2008).[25] Interestingly, the announcement of new sanctions by the White House Press Secretary included this statement:

> *"As the President has said, our response to North Korea's attack against Sony Pictures Entertainment will be proportional, and will take place at a time and in a manner of our choosing. Today's actions are the first aspect of our response."*[26]

Apparently, the option of a cyber counterattack remains "on the table." As Navy Captain Joel Doolin noted during his presentation, the January 2015 EO constituted the "first exercise of national instruments of power (diplomatic, economic, information) in response to a cyberattack."[27]

In late February 2015 (after the policy workshop was held), a Presidential Memorandum was released, outlining the establishment of a Cyber Threat Intelligence Integration Center (CTIIC) under the office of the Director of National Intelligence (DNI). The CTIIC

is, according to this document, to include representatives from "all executive departments and agencies," with a mission "to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests [including critical infrastructure components] using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities." As specified, the CTIIC is to have reached "full operating capability by the end of fiscal year 2016."[28] This new attempt to protect key elements of national infrastructure may yet prove to be the elusive policy measure needed to fill the gaps noted in the protection and defense of these, possibly the most grave, vulnerabilities.

An additional Presidential act that occurred following the workshop was an April 1st (2015) White House declaration of a "national emergency" via an EO designed to impose sanctions on "Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." A statement within the EO proclaimed that this action was "intended to 'fill in a gap' that exists between the law-enforcement and diplomatic means currently available to pursue malicious hackers,"[29] but it is noteworthy that neither non-cyber military means nor cyber response were mentioned as currently available options. Only time will tell if a threat of sanctions and/or economic restrictions will actually work well as a deterrent.

Representatives of breakout groups cited a generic lack of congressional engagement in cyberspace issues. This was addressed by Congressman Scott Perry (during a skyped question and answer session), who sits on several committees that touch on cyber topics, the most relevant being the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, House Homeland Security Committee. Participants noted with concern that services and agencies lack sufficient authorities needed for future cyberspace operations at the operational and tactical level, as authorities currently exist only at the highest levels of government.

Attendees generally agreed that cyberspace operations should be part of integrated fires and rules of engagement at the onset of hostilities; but differences in service-specific training and manning levels as well as variances in cyber-related operational approaches reveal a potential for chaotic joint action, at least in the early stages of a conflict. Given the

expectation of compressed timing in cyberwarfare, and especially under a "first strike" scenario, the cost of such chaos may be extremely high.

Also cited by attendees during the Congressman's session was the lack of adequate liaison assignments for representatives from service headquarters to assist Congress with service-specific cyberspace mission requirements. An absence of consistency among the services in how or whether members have opportunities to learn about and/or participate in the policy process may partially account for the problem. A few senior military and civil service participants commented that an institutional reluctance (the level of which is service specific) to tackle policy issues and assist policymakers on their turf seems only to result in increases in the number of gaps and vulnerabilities, and exacerbate the tension between policymakers and those who must comply.

Finally, members of the breakout group tasked with examining the international perspective as it pertains to cyber policy discussed the absence of international norms. They indicated that each nation-state has a discernible set of general values and cultural aspects which influences regard for privacy, freedom of speech, and asset ownership. Considering the absence of a consensus on norms across the international community to be a critical gap, they suggested a need for an international convention to establish a framework for addressing cyberspace issues in the global arena.

**Responsibilities**

Participants in each of the three breakout groups (focusing on the international/global arena, security and defense of the homeland [public and private], and national security/DoD concerns and requirements) included doctrinal experts as well as lawyers, who provided extensive clarification throughout the proceedings. Their input was crucial to understanding the current basis of action and non-action within each area of concern.

Within DoD, cyber-security policy was assigned to the Assistant Secretary of Defense for Homeland Defense (ASD/HD) as part of former Secretary of Defense Hagel's restructure. The fact that the latest ASD/HD nominee (as of February 2015) was Eric Rosenbach, who has an extensive background in cybersecurity and had previously held

the position of Deputy Assistant Secretary of Defense for Cyber Policy, underscores the importance placed on cyberspace with regard to the role of DSCA and other cyber responsibilities of the National Guard.

In the homeland defense and national security arenas, U.S. government agencies with key cyber security and cyber policy responsibilities are DHS, DoD and DOJ. Upon cursory examination, it would appear that cybersecurity duties have been delineated: DHS has been assigned as "lead" for cybersecurity, DoD's mission is defense of the nation from external threat, and DOJ is the "go to" organization for investigations and law enforcement. The application of structure to reality, however, is more complicated.

According to DHS's Office of Cybersecurity and Communications, DHS coordinates national protection, prevention, mitigation of, and recovery from cyber incidents and protection of critical infrastructure as well as the security of civilian computer systems at the federal level (.gov). The mission of DoD is that of *support* to national protection, prevention, mitigation of and recovery from cyber incidents. [30]

The 2015 DoD Cyber Strategy (*a later version of the DoD Strategy for Operating in Cyberspace*) identifies "three primary cyber missions" for the Cyber Mission Force:

- Defending "DoD networks, systems and information"
- Defending "the U.S. homeland and U.S. national interests against cyberattacks of significant consequence"
- Providing "cyber support to military operational and contingency plans"[31]

*Joint Publication 3-27: Homeland Defense* and *Joint Publication 3-28: Defense Support of Civil Authorities* recognize DHS as the agency tasked with "protect[ing] the United States and its people, vital interests and way of life." DoD's HD mission is the "protection of U.S. Sovereign territory, the domestic population, and critical infrastructures against external threats and aggression, or other threats as directed by the President." Defense Support of Civil Authorities (DSCA) is assistance provided by DoD to and in support of domestic civil leadership.[32]

Although there are known to be "overlapping roles, responsibilities, authorities, and capabilities,"[33] associated with the DSCA mission, and

coordination is evident, workshop participants indicated that there remains much room for confusion overall, allowing for the occasional denial of responsibility. A lack of specific tasking – and thus a dearth of resources – can leave command and control in question.

Activities in cyberspace have advanced to the point where virtually all public, private, and individual interests are based upon and/or controlled by circuits and software. Thus, all sectors are dependent on the safety and security of the cyber realm. The government is generally responsible for security and defense missions, but identification of responsibilities is not easy. Ever-increasing global use and disruption capabilities have made decision-making with regard to the distribution of authorities over aspects of cyberspace requiring stability for the continued functioning of society and the maintenance of sovereignty extraordinarily difficult. The pace of technological development further frustrates efforts to corral the cyber problem within traditional bureaucratic stovepipes.

Mission allocation adhering to organizational and geographically-defined (sovereignty-based) norms may have initially seemed, at least to the politicians involved, to be an obvious and easy way of tasking and assigning the various aspects of cyberspace operations. Nevertheless, workshop participants concluded that while fixed assignments of cybersecurity and defense authorities may have precluded some overlapping functions, a consequence of that success has been progressive revelation of gaps in defense and an increase in systemic vulnerabilities that imperil national security. Defense-in-depth, digital and non-digital, suffers.[34]

Public and private sectors attendees agreed that budgetary restrictions, limited resources, the ongoing development of a legal framework, and either vague or very specifically focused regulatory/legislative delineations of responsibilities exacerbate full-spectrum cyber defense. The results include creation of the potential for repudiation of responsibilities in the public sector, and denial (by legal means via the Criminal Fraud and Abuse Act [CFAA][35]) of the private sector's opportunity to respond. There is an overall lack of coordination; and the points at which the transfer or handoff of responsibilities must be made, as well as the processes for transfer to be followed, are not clearly

defined within DoD or across the Interagency. The consequence of confusion is a lack of, or (alternatively) weak or otherwise ineffective action. Group representatives identified these factors as highly problematic with regard to the protection and defense of critical infrastructure, and potentially catastrophic in respect to sovereignty.

Attendees took note of international law and treaties regarding use of force, as well as "proposed" or non-binding documents such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[36] The *Tallinn Manual* was the product of a three-year project designed by the NATO Cooperative Cyber Defence Center of Excellence. Described by the project director as "an expression solely of the opinions" of a chosen panel of experts, it has credence as a creative attempt to apply international law to cyberspace. Although controversial, and neither comprehensive nor official, the *Tallinn Manual* provides a foundation for further deliberation.

In 2012, State Department legal advisor Harold Hongju Koh, while at a USCYBERCOM Inter-Agency Legal Conference, stated emphatically "that established principles of international law do apply in cyberspace." Koh explained that cyber operations could "in certain circumstances," be "use of force within the meaning of Article 2(4) of the UN Charter and customary international law." He further noted that nation-states are legally responsible for events caused by state-sponsored cyber actors; yet he recognized the problems associated with attribution.[37]

Citing three major critical infrastructure incidents where "the same kind of physical damage that dropping a bomb or firing a missile" would occur as examples of "use of force" in the cyber realm, Koh affirmed the national/sovereign right to self-defense under Article 51 of the UN Charter. He additionally reasoned: "states conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict." Systems that make up networked infrastructure are most often located within the bounds of a sovereign state, and thus "subject to the jurisdiction of the territorial State." Operations targeting such infrastructure could create both desired effects and unintentional consequences within the territorial state and beyond, due to the nature of the net.[38]

Other legal experts (including some attendees with backgrounds in law) tend to consider the implications of cyberspace to established law as a more complex problem set. Captain Doolin cited Koh in his plenary presentation under the heading of "trying to fit the square peg of cyber into the round holes of existing constitutional and international law."[39] An article by former Senior Advisor to the Director of National Intelligence and Cyber Coordination Executive Melissa Hathaway, addressing the challenges of sovereignty within a "multidimensional" cyberspace environment, was another source of discussion. Ms. Hathaway identified the need for "an appreciation of the entangled economic, technical, regulatory, political, and social interests implicated by the Internet" when considering an increasing struggle for "power and control over all aspects of the Internet and Internet economy."[40]

Deliberations of cyber within currently accepted law, internationally and domestically, becomes more nebulous (and thus more difficult to garner consensus) when public and private needs are incongruent, or worse – diametrically opposed. Within the United States, the cyber threat has magnified the differences between protection of all facets of government and protection of business continuity (physically and economically). It has also underscored government reliance on the private sector (e.g. for critical infrastructure and services) and vice-versa. Ensuring that legislative and regulatory initiatives intended to cover the cyber arena do not cause harm to one sector at the expense of the other is reportedly a constant concern.

## The Question of Sovereignty

Over the course of this three-day workshop, participants – as experts in differing areas of the cyber problem – considered the objectives and research questions within the context of "cyber sovereignty." It was ultimately the opinion of all groups that the problem set actually pertained to matters involving national sovereignty; thus negating the use of the label "cyber sovereignty." Discussions thereafter focused on the need to examine the implications of cyberspace to the structure and maintenance of national sovereignty.

Conversations included questions regarding the critical infrastructure elements considered crucial to the continuity of national sovereignty.

An article provided to participants for discussion, "Sovereignty in Cyberspace: Can it Exist?" by Lt. Col. Patrick Franzese, addressed the catastrophic aspects of cyberattacks on civilian and military targets to key elements of critical infrastructure.[41] He described the current state of cyber "standoff" (or non-response) as a hindrance to the potential establishment of "sovereignty in cyberspace." He further cited the reluctance of U.S. officials to discuss cyberattacks openly for fear of acknowledging that an "act of war" may indeed have occurred without efforts or ability (considering attribution difficulties) to retaliate.[42]

Participants noted that banks, corporations, utilities, and other private sector businesses are also reluctant to report cyberattacks, because of negative connotations, which could make or break a business.[43] In 2011, the Securities and Exchange Commission (SEC) issued guidance in an attempt to explain obligations of cyber incident disclosure in accordance with existing federal securities laws. The guidance seemed to have been written more as a non-binding sympathetic delineation of risk, however, as it stated from the outset that it "is not a rule, regulation, or statement of the Securities and Exchange Commission…[and] the Commission has neither approved nor disapproved its content."[44]

As the SEC considers more explicit rules on disclosure specific to publicly traded corporations, business is pushing back. The U.S. Chamber of Commerce argued that mandatory disclosure would not only exacerbate the threat (it "could paint a target on registrants' backs"), but could irreparably damage profits and therefore the continued viability of the company.[45] Still, reporting of large-scale attacks that effect a company's revenue or result in a loss of customers' personal information is becoming more common. With hackers exposing exfiltrated data on the web (or "darknet") for all to see, it is becoming harder for victimized businesses and organizations to keep silent about attacks.[46]

Soon after the Chamber of Commerce expressed their concerns, Congress deliberated an addition to the National Defense Authorization Act (NDAA) which "would enhance cyberattack reporting requirements for large defense contractors," focusing on those that are "operationally critical." Although most private companies, to include large defense contractors, welcome opportunities to share cyber threat data in theory,

they fear wider government disclosure, which would expose them to extensive litigation.[47]

While Congress has expressed a willingness to explore legislation providing liability protection for industry specific to cyberattack disclosure, there is another matter that needs immediate attention – that of response. Legal experts and business representatives who participated in the workshop noted (with some exasperation) that the CFAA criminalizes self-help countermeasures by private entities.[48] If a business cannot legally respond to attacks against it, what recourse does it have? Certainly, cyber attackers – domestic or international – do not appear dissuaded by the CFAA.

A few days following workshop proceedings, Richard Turner, FireEye's Vice President for the Europe, Middle East and Africa region, told *Newsweek*: "In addition to spending money to prevent attacks, companies must have the mindset that breaches are inevitable, and they've got to be able to identify breaches quickly after they have occurred and then launch a proportionate response."[49] Turner did not seem to be advocating the same kind of response that U.S. government entities have advised to this point (the legal kind) – that of identifying, containing, reporting, and (if possible) bringing civil action against the perpetrators[50] – but then, he was speaking to an international audience. Does extraterritorial counterattack by non-American enterprises leave U.S. businesses hamstrung or does it keep U.S. businesses from unintended consequences that could include starting a larger conflagration? Unfortunately, as workshop participants noted, the answer is yes to both questions. This is the type of cyber dilemma that holds policy creation and resolution at bay.

**Shift of Focus from National Security to National Defense**

One of the most perplexing cyber issues of our time has been the question of when cyber threats and adversarial cyber activities shift from a matter of national security to that of national defense. An article entitled "Perspectives for Cyber Strategists on Law for Cyberwar" by Major General Charles J. Dunlap Jr. (USAF, Retired)[51] provided attendees with a basis for consideration of this quandary.

Is the law of armed conflict (LOAC – a.k.a. international humanitarian law) applicable to cyber threats? Having acknowledged that legal opinions regarding the adaptability of current international law to the cyber problem differ, Dunlap warned against attempts to establish international clarity – "once an international norm is established, it forever after can be a legal impediment."[52] Workshop participants further asserted that international norms are often upheld by only one side of a conflict.[53]

Dunlap's article explored the difference between cybercrime as a law enforcement issue and cyberattacks as a national security/national defense problem.[54] In the cyber realm, cybersecurity is necessary to national security, and the nature of attack (whether criminally or militarily invoked), although highly relevant to response, is irrelevant to the necessity of implementing sound security measures. Cyber defense, on the other hand, is within the national defense arena and specific to the mission of government and the military. While often used interchangeably, participants upheld that cybersecurity is focused on matters designed to maintain the viability of the network as well as systems that comprise it, and is everyone's responsibility (public and private); while cyber defense would include all options. Cyber defense begins with cyber security, but given appropriate authorities under a defined set of circumstances, can be elevated to cyber response.

Workshop participants discussed a reticence to step beyond the ever-increasing need for cyber security. As previously noted, it is illegal for private corporations to respond to cyber events in any way that might be interpreted as an attack or counterattack against presumed perpetrator(s). It is also illegal for civilians employed by – even though acting on behalf of – government organizations to do so. Furthermore, as Dunlap noted, debate continues over the meaning of Article 51 of the U.N. Charter (which allows for national self-defense only if responding to an "armed attack") in the context of cyber hostilities.[55] Thus, other than an increasing cost for security, there would seem to be no recourse for escalating risk, soaring losses, and growing complexity of cyber events.[56]

Still, defense and law enforcement sectors both readily acknowledge the need for collaboration with business to avoid "catastrophic

cyberattacks."[57] The consequences of cyber infiltration of civilian-owned critical infrastructure and other key resources can be just as dire (and possibly more so) as cyberattacks aimed specifically at government and/or military systems. Motivation was, until recently, a differentiating factor between attacks on public and private sector systems. This no longer seems to be the case. Increased capabilities and growing alliances of cyber adversaries are making it possible for methods, means, and even motivations, to merge.[58]

Attendees referred to a report by Aljazeera America only a few days prior to the workshop concerning the discovery of BlackEnergy malware (believed to be of Russian origin) and the implication that it "could be used to sabotage America's most critical infrastructure." The Aljazeera article quoted David Smith, Director of the Potomac Institute Cyber Center, as saying:

> *"There is no benign explanation for why somebody in Russia is interested in how the lights go on and off in Ohio.… If you're asking me, is somebody preparing the battlefield against the United States and its allies? You bet somebody is."*[59]

Does the insertion of malware that could potentially harm critical infrastructure (and thus cause destruction roughly equal to kinetic effects) rise to the level of an "armed attack" or an "act of war?" Could a cyber first-strike capability involving the strategic deployment of malware be likened to the events surrounding the Cuban Missile Crisis? If so, is pre-emptive action justified?

These questions are, of course, open to legal debate – and it was not the objective of the workshop to determine specific answers to this type of question. Dunlap, however, provided "the leading view" of experts regarding cyber applicability to Article 51 of the UN Charter, which took note of certain types of cyber actions (or cyber "weapons") which would qualify, if and/or when used, as an "armed attack" due to the nature of effects that would result from their use. A qualification for response, Dunlap notes, is that the source of hostilities must be identifiable as acting at the behest of or under the sponsorship of a nation-state,[60] or alternatively as a cyber equivalent of an "organized terrorist enemy."[61] Unfortunately, as participants pointed out, attribution of hostile acts in cyberspace is difficult, at best – and even

more so when a nation-state uses cyber-proxies posing as criminals. Dunlap summed it up rather well with this statement: "The identity of the attacker may well determine if a state of war exists."[62]

It is therefore presumed (and was generally agreed upon by workshop attendees) that within the United States, a publically recognized shift in focus from national security to national defense in the context of cyberspace would come down to the declaration of an act of war, or acknowledgement from the President that an armed attack from a hostile source had occurred. Major General Dunlap identified the phrase "act of war" as political, vice legal terminology,[63] and legal representatives at the workshop concurred – with regard to potential U.S. military/government response, the President is the only entity who can declare that a cyber event is actually a "cyberattack."

Compounding the problem of transition from national security to defense is the diffusive nature of attacks and of cyberspace infrastructure. Attribution is delayed because, like an army of ghosts,[64] attackers can and do deflect their presence to a myriad of global locations, using hijacked systems. This gives rise to even more unresolved questions:

- Should nations in which cyber infrastructure is used for an attack be held responsible?
- If so, what are the implications for cyber response?

Another concern noted is that we may be near, or already engaged in, a less-publically acknowledged "cyber cold war,"[65] where "some states appear quite content to err on the side of boldness," operating with an assumption that "actions [in cyberspace] do not carry real-world consequences." Recognition of the potentially dire consequences has led to calls for "respecting one another's virtual sovereignty" and a more aggressive rhetorical stance by U.S. leadership;[66] but for the moment, players in this game "appear to be testing the boundaries in cyberspace, safe in the knowledge that those boundaries are undefined."[67]

Workshop participants agreed that the United States must be prepared to back up rhetoric with action for full effect. They also stressed that once laws are solidified, the United States must operate under the knowledge that it will, as in counterterrorism efforts, be held to international scrutiny beyond the levels afforded to adversaries, as well as allies in cyber conflict.

It takes a great deal of time for intelligence collection, attack analysis, attribution, and the ultimate political deliberation (which should include consideration of civil liberties) to result in decisions that might involve operational response. Participants generally viewed defensive measures as useless if authorities are unable to initiate timely response to a catastrophic cyberattack, especially if adversaries launch subsequent, follow-on attacks (cyber or kinetic). Essentially, this "cyber first-strike" scenario against the United States dictates that victims are sitting ducks with a predetermined destiny of destruction.

**Recommendations**

Breakout groups identified immediate needs for the DoD. These included necessity of a better definition as well as more latitude and authority with regard to recognition of an official "cyberattack." There was additional agreement that the National Security Council (NSC) should create more definitive policy and instruction concerning recognition and/or identification of a "cyber act of war."

It was agreed that legislation was needed to clarify and improve the efficacy of DoD's role in domestic and international support with regard to potential cyber hostilities. One suggestion – that of the establishment of a principal cyber advisor as a staff element for doctrine and policy – might help.

As there are no pre-scripted Defense Support of Civil Authorities (DSCA) Cyberspace missions, it was recommended that the Joint Staff explore specific policy for a DoD mission to deter and defend against malicious cyberspace activity by non-U.S. persons directed at critical infrastructure and resources. This would necessarily include identification and removal of obstacles that encumber DoD planning to respond to a domestic cyber incident. Issues that still need clarification include:

- At what point does the "hand-off" between law enforcement and DoD/Intelligence occur (e.g. when is theft declared an "attack" [in the layman's sense of the term, as only the President can declare whether an "attack" has occurred])?
- What are the lines of demarcation between cyber security, cyber defense, and cyber operations? Are partitions flexible, decided

according to threat actors and levels? If so, who makes the decision to switch from one to another?

- What is "proportional response" in cyberspace? Have regulations limited proportional response in cyberspace to the extent that any response (other than increased security) is ineffective or ill-advised?
- What is the threshold for escalating response? Can specific trigger events be identified?

Acknowledging differences between services in expectations and ability to participate in policy development at all levels, workshop attendees believed there to be a need for and approval of more participation by all DoD elements, especially with regard to the cybersecurity and cyber defense missions. Experienced DoD personnel can provide a perspective crucial to the creation of sound legislation.

DoD-specific recommendations included the establishment of contracting requirements for minimum cybersecurity standards (i.e. DISA/NSA IA Standards) by the Joint Chiefs of Staff (JCS). Joint training and certification standards for cyber operators as well as a Joint manning document are necessary for a Joint Cyber Headquarters. Exercises involving unified action should be required and cyber scenario interagency wargaming for incident response must be more robust and expanded to include participation of representatives from the private sector. Services need to expand Innovative Readiness Training (IRT) to include cyberspace operations and hold community of interest conferences for operations, plans, policy, and legal synchronization.

Attendees commented that the Secretary of Defense (SecDef) and/or the JCS should increase DoD capability/capacity for cyberspace defense and provide for the development of a cyberspace operations pilot program for surge operations. Furthermore, participants advocated for the delegation of authority for execution of response options to lowest practical level – preferably to the command or tactical level.

Breakout groups considered several policy additions and changes, including the following proposed policy statement:

> *"The [United States] will promote and support international norms of conduct in and among members of the international community to ensure mutual respect for, and security of, those activities in,*

> *and components of, cyberspace commensurate with traditional rights of sovereignty, as related to territorial integrity, political independence, and U.S. core values and national interests."*

In support of the above proposal, participants suggested that the U.S. Government (presumably the State Department) promote the concept of an international convention on cyberspace for the deliberation and adoption of international norms.

One of the most notable legislative recommendations pertained to the enactment of a "Cyber Sarbanes-Oxley Act"to increase accountability with regard to critical infrastructure stakeholders in the private sector.[68] This would necessitate mandatory (for key resources) and incentivized reporting and compliance as well as the sharing of cyber threat information between the public and private sectors.

To that end, continued legislative refinement of authorities to enhance sharing of information at all levels (local, state, federal and industry) is needed. In order to more effectively improve data sharing between public and private sectors as well as allied and coalition partners, participants cited a need to seek greater understanding of private-sector equities and needs which currently inhibit information sharing. Limited liability protections could be (and will no doubt need to be) invoked in order to encourage greater sharing of information.

Discussion of data sharing invariably brings up the need to improve intelligence support to state and local governments as well as law enforcement and industry. Greater authorities are required to collect real-time threat information while protecting civil liberties. The identification and adoption of changes in communications and information systems during or after a "cyber crisis," and ultimately, increased capabilities to determine attribution in cyberspace are necessities.

Some asserted a need for new policy governing unconventional cyber warfare in light of a multitude of recent highly sophisticated threats from a variety of sources aimed at destruction of data and property. A unique example given by attendees of unconventional cyber warfare – that of hostilities associated with two non-state actors or groups fighting in cyberspace (e.g. Anonymous vs. Cartel) – not only raises

questions of authorities and responsibilities, but invites consideration of collateral damage (digital and physical) in determination of policy.

Because of the immense financial burden placed on the private sector incurred by cyberattacks, theft, and need for constant enhancement of cybersecurity, participants saw a need to decriminalize private-sector "self-help" response options. This is an extremely controversial remedy; but with appropriate controls and oversight, private sector support against cyberattacks could work to the benefit of national security and national defense.

Workshop representatives of the legal profession commented that the Clinger-Cohen Act of 1996 is in need of attention, as there have been no updates since cyberspace received a "domain" designation. The Clinger-Cohen act focused on information technology (IT) "investment" (formerly acquisition) and IT resource management to include analysis and evaluation of risk. It also established the office of Chief Information Officer (CIO) within agencies to report on efficiencies.[69] Critics claimed that it sacrificed security for economy, allowing long-held practices of comprehensive risk-aversion to be replaced by business logic associated with the practice of risk management. Considering the devastation that cyberattacks are now capable of producing, a complete lack of control over the systems (technology) production process, and the fact that malware is almost ubiquitously embedded within system components as they are produced and sold, workshop participants strongly suggested that it is past time to update the Clinger-Cohen Act.

One breakout group reviewed *Homeland Security Policy Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD – 7), which acknowledges that key segments of critical infrastructure are "so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating impact on [national] security and economic well-being."[70] The group recommended amending or rewording portions of HSPD-7 to underscore the importance of deterrence and defense of critical infrastructure as well as consequence management. They proposed a revision (see below) to provide the directive with stronger language and an improved capacity for relevant organizations to respond to significant hostile cyber acts against critical infrastructure.

Recommended HSPD-7 Policy re-wording:

From:

- It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:
  - Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction
  - Impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety
  - Undermine State and local government capacities to maintain order and to deliver minimum essential public services
  - Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services
  - Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources
  - Undermine the public's morale and confidence in our national economic and political institutions

To:

- It is the policy of the DoD to deter and be prepared to defend [and support consequence management] from cyberspace attacks [by non-U.S. persons] that have the potential to:
  - Disrupt, degrade or destroy U.S. or allied military capability
  - Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction
  - Significantly impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety
  - Significantly undermine State and local government capacities to maintain order and to deliver minimum essential public services
  - Significantly damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services

– Have a significant negative effect on the economy through the cascading disruption of other critical infrastructure and key resources

Overall, changes need to be made with a "whole of government, whole of community, whole of nation" approach to security, defense, and sovereignty within the context of cyberspace while encouraging (and mandating only when necessary for matters of national defense) input and participation from the private sector. Regardless, the government should regularly consult private industry, even if only to determine unintended consequences.

**Conclusions**

Extensive discussion on gaps and vulnerabilities led to a consensus on existing gaps in national policy, with recognition that further contemplation of strategy and operations is necessary to consider this a comprehensive examination. Coordinated proposals submitted by participants summarized their understanding of how to best confront legislative challenges for the maintenance of sovereignty in cyberspace.

Key recommendations included:

- The identification and removal of obstacles that encumber DoD planning to respond to a domestic cyber incident
- More DoD participation in cyber policy development at all levels
- The necessity for the enactment of a "Cyber Sarbanes-Oxley Act" (to increase accountability with regard to critical infrastructure stakeholders in the private sector)
- A rewording of Homeland Security Policy Directive 7 (HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection)
- A need to update the Clinger-Cohen Act of 1996 (which focused on IT investment and resource management)

In testimony before the House Subcommittee on Emerging Threats and Capabilities, Admiral Michael Rogers (Commander, USCYBERCOM) indicated that "potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our

homeland is at risk if tensions ever escalate toward military conflict."[71] Only a few months prior to the Admiral's statement, DHS released information about a Trojan Horse (malware) identified as "BlackEnergy, believed to have originated with Russian government-sponsored hackers…[and] designed to target critical energy infrastructure."[72]

Former Secretary of Defense Leon Panetta,[73] former CIA Director Michael Haydon,[74] and former Secretary of Homeland Security Janet Napolitano,[75] have also warned that a cyberattack against the electric grid could be devastating. It is worth noting that the Russians have already used cyber effects at the onset of hostilities[76] and that terrorists have already targeted critical electric infrastructure in other countries.[77]

Given the fact that hostile cyber acts against U.S. systems are occurring in vast numbers on an hourly basis, and that the precedent has been set for a cyber "first strike," it seems inevitable that a major cyberattack will preface any kinetic effort launched against the United States. There is no doubt that this would be a key way for adversaries to improve their odds.

Workshop attendees maintained that reliance on historical doctrine and static context is unacceptable given the numbers and affiliations of potential adversaries as well as the enormously complex nature of current adversarial intent. An immediate, comprehensive effort is necessary to illuminate the context within which the proverbial "first battle of the next war" will most probably be fought.

Author John Shy, in *America's First Battles: 1776-1965*, claimed: "the first battle almost guarantees that inexperience will be paid for in blood."[78] Could the 21st century cyber equivalent to "inexperience" be a lack of attention to the formulation of sound policy, strategy, and doctrine?

# Chapter 2: Strategy

## General Overview

The first Cyber Sovereignty Workshop (Policy focus) revealed confusion with regard to authorities and missions, vague and inadequate policy, gaps in relevant international and domestic law, and insufficient doctrinal development. There was great concern by both public and private sectors over a lack of holistic, "whole of community, whole of nation" strategy for unified action in exercises, wargaming, and incident response.

Secretary of Defense (SecDef) nominee Ashton Carter, in his response to questions posed by the Senate Armed Services Committee only a week before the first workshop, spoke of a need for a holistic cyber strategy "utilizing all means at the government's disposal to deter and respond to cyber threats." Carter further noted:

> *"Deterrence cannot be achieved through cyberspace alone, but requires a multi-faceted effort across the totality of the U.S. Government's instruments of national power, including network defense measures, economic actions, law enforcement actions, defense posture and response capabilities, intelligence, declaratory policy and the overall resiliency of U.S. networks and systems."*

Carter's solution was a "whole-of-government approach," which included the Department of Defense (DoD), Department of Homeland Security (DHS), Department of Justice (DOJ), and the Intelligence Community (IC), "as well as with other federal partners."[1]

A report published by the IBM Center for the Business of Government and the Computer Science Department of Indiana University of Pennsylvania a few days prior to SecDef's written testimony also stated a need for a broad approach to developing a strategy.[2] Participants in the roundtable upon which the report was based warned: "When authorities do not provide safety for those in jeopardy, unofficial

groups might emerge to provide a physical (or cyber) response."[3] Yet these academics and private sector representatives, who recommended government action while heavily emphasizing critical infrastructure, failed to suggest the role that private sector organizations should play in the development of cyber strategy.

The government (all levels) depends on private sector businesses and infrastructure. Furthermore, healthy critical infrastructure (especially the electric grid, communications and transportation) is crucial to the maintenance of civil order and ultimately to sovereignty. Yet, until recently, corporate cooperation with government entities regarding cyber issues was associated with "high-risk." Private sector executives "fear[ed] the collateral consequences of involving the government in cyber incident response."[4]

Judith Germano, of New York University's Center on Law and Security, highlighted barriers to public-private cooperation (legal and otherwise) on cyber problem sets in her October 2014 publication entitled *"Cybersecurity Partnerships: A New Era of Public-Private Collaboration."* Acknowledging the need to change, she stated:

> *"Because significant access, expertise, and perspective needed to address the cyberthreat reside in both the private and public sectors, and because the law in this area is unsettled, collaboration is essential to attain feasible and effective cybersecurity solutions. It is also important for the private sector to be significantly involved in the development of the legal regime regarding cybersecurity or we risk ending up with laws that cannot be implemented as envisioned."*[5]

Participants (public and private) at the second Cyber Sovereignty Workshop (Strategy focus) were not reticent to acknowledge the need for private sector participation. They inherently understood and sympathized with Ms. Germano's perspective and agreed with the IBM report's consideration that "an out-of-control escalatory spiral" could occur "absent a commonly understood definitional framework to help frame strategic and tactical choices."[6] Due to military and government reliance on privately-owned critical infrastructure, as well as the fact that attacks on private sector targets can be equally (or more) devastating to national security,[7] it was realized that failure to include private sector

in the strategy development process could ultimately result in failure to protect and defend the nation.

Thus, SecDef Carter's "whole-of-government approach" needs to expand to "whole-of-community" and "whole-of-nation" (assuming "whole-of-government" would fall under "whole-of-nation").[8] Participants at the first Cyber Sovereignty Workshop recommended a similar approach that included private sector input and assistance. As USCYBERCOM Commander Admiral Michael Rogers noted: "The public and private sectors need one another's help."[9]

On June 23–25, 2015, the Mission Command and Cyber Division, Center for Strategic Leadership, U.S. Army War College (USAWC), in partnership with United States Cyber Command (USCYBERCOM), and United States Army Cyber Command (ARCYBER) conducted an unclassified workshop entitled "Cyber Sovereignty: Strategy." This workshop was the second of three dealing with the fundamental issue of sovereignty in the context of cyberspace. In response to SecDef's complaint about the lack of a "holistic cyber strategy" and with respect to deliberations on policy within the first Cyber Sovereignty Workshop, participants were asked to consider the need and develop a framework for a holistic ("whole-of-community, whole-of-nation") national cyber strategy.

## Objectives

The determination of what constitutes cyber sovereignty in the policy and strategy realms will greatly influence identification and understanding of threats, DoD and IC preparation of the battlefield, the development of capabilities, and strategic planning for cyberspace operations. Participants in the first Cyber Sovereignty Workshop noted gaps in policy with regard to international and domestic law. Those attending the second worked to verify a requirement for a holistic, or "whole-of-community, whole-of-nation" cyber strategy, and to produce a basic framework for initial consideration.

A strategy for protection and defense of DoD, state, local, and federal governments as well as dual-use private sector cyberspace activities and functions may be necessary to minimize confusion in the decision-making process and define the rules of cyberspace engagement. The primary objectives for the June (2015) event were:

- To review and consider the outcome of the Cyber Sovereignty Policy Workshop (February 2015), using results and recommendations as background for the Strategy focus workshop
- To determine a requirement for and (if validated) ultimately establish a framework for a holistic national cyber strategy for protection and defense of DoD, state, local, and federal government as well as dual-use private sector cyberspace activities and functions – a "whole of community, whole of nation" National Cyber Strategy, looking at ends, ways, and means
- To recommend which government and non-government organizations are or should be participating in developing a comprehensive cyber strategy

**Research**

Participants examined the following documentation in preparation for the workshop:

- *The National Strategy to Secure Cyberspace* (February 2003)[10]
- *Department of Defense Cyber Strategy* (April 2015)[11]
- The *National Security Strategy* (February 2015)[12]
- *International Strategy for Cyberspace* (May 2011)[13]
- The National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014)[14]
- A report entitled "*Developing a National Strategy for Cybersecurity*" (October 2013)[15]

Research questions derived from the aforementioned objectives were offered for discussion and strategy formulation purposes. Attendees addressed questions to the extent possible in an unclassified environment. Points of consideration included:

- What policy shortfalls discussed in February create impediments and/or obstacles to the development of a national cyber strategy?
- What cultural changes are needed to meet security and defense challenges within cyberspace? Leadership competencies?

- What current strategies are in place with regard to national defense and security (DoD, State, Local, Federal, and dual-use private sector resources) in the maintenance of U.S. sovereignty in cyberspace?
- What global strategic cyber issues should a National Cyber Strategy include?
  - Do the current and recently published strategies (e.g. *National Security Strategy*, *DoD Cyber Strategy*, and the *International Strategy for Cyberspace*) attempt to alleviate the shortfalls in policy?
  - Are the published strategies applicable in lieu of the policy gaps established in the February workshop?
  - Do the new *National Security Strategy* (NSS) and the *DoD Cyber Strategy* meet the requirements for national sovereignty?
- Who are U.S. cyber adversaries (current and future)?
  - How do adversaries resource and utilize cyber forces?
  - Are adversarial cyber intelligence operations an impediment or threat to national sovereignty?
  - Will cyberspace response to criminal and/or adversarial acts by non-government actors undermine sovereignty?
  - How could non-governmental actions in response to threat effect deterrence and/or war termination efforts?
- Are there cyberspace scenarios where a "first-strike" could effectively dissolve or destroy the bonds of national sovereignty and thus "lose the war" without ability to respond?
- What strategic preparation of the operational environment should be made in consideration of recent and current cyber events?

Participants were representative of the same organizations and sectors as those invited to the first workshop, and many individuals were attendees of both events. The returning participants provided a backdrop of knowledge concerning deliberations that occurred in February, and came armed with valuable perspectives on recently reported cyber exploits.

Facilitators asked breakout groups to concentrate discussions as follows:

- Private Sector: What are the implications and concerns in the private sector with regard to the development of a National Cyber Strategy?
- Interagency: What are the responsibilities of Interagency organizations in the development of a National Cyber Strategy?
- National Security Council: Considering current policy, what are the national issues with regard to the development of a National Cyber Strategy?

**Group Deliberations**

A requirement for a holistic national cyber strategy for protection and defense of DoD, state, local, and federal government as well as dual-use private sector cyberspace activities and functions was considered and established as necessary. The consensus of all breakout groups was that existing documents were either obsolete or insufficient. Some participants maintained that the *National Security Strategy* (NSS) should cover the realm of cyberspace, while others feared that the NSS, as written, is deficient in a "whole of community, whole of nation" context, and asserted that it depends largely on cybersecurity and law enforcement (passive cyber defense). In fact, many attendees argued that the NSS was more of a communication of "ends" than of "ends, ways, and means." Still, they generally agreed that a National Cyber Strategy should be "anchored with" the NSS.

Participants noted that the verbiage within the section of the *National Security Strategy* focusing on U.S. leadership only briefly addressed cyber issues.[16] They suggested that a holistic cyber strategy must state the need for the United States to secure leadership in the cyber domain in order to protect sovereignty, defend constitutional rights (including privacy), and maintain an open and interoperable Internet.

Beyond establishing the requirement for a National Cyber Strategy, deliberations led to recommendations for organizational/functional participation and roles (including a collective capacity to act) in strategy framework formulation. Throughout the proceedings, participants emphasized that extensive collaboration between public and private sectors is key to development of a comprehensive and relevant final effort.

Organizational Participation/Stakeholders should include:

- All federal Executive departments and agencies
- State, Local, Tribal, and Territorial governments
- Private sector (including, but not limited to, Critical Infrastructure/ Key Resource [CI/KR] owners and operators)
- Foreign Partners
- Academia

The inclusion of all cyber stakeholders – especially the private sector – is essential to the success of the strategy.

Although the workshop focused on the development of a National Cyber Strategy, international applications were points of discussion. Participants reviewed the President's 2011 *International Strategy for Cyberspace*,[17] noting similarities in tone with the *National Security Strategy*. They proposed for the record:

> *The United States must encourage an international cyberspace effort that promotes security and economic prosperity on a global basis, and assists with the establishment of an international capability to address challenges to national security in the cyber arena.*[18]

Discussions about principal guidance for a National Cyber Strategy stressed the maintenance of shared, connected space, with additional emphasis given to information as a national asset to be both shared and safeguarded. Breakout groups also discussed the possibility of extensive cyber education, determining that to be fundamental to effective cybersecurity and cyber defense by both public and private stakeholders.

**Recommended Framework**

**Proposal**: This proposal is for a National Cyber Strategy, anchored to and by verbiage in the *National Security Strategy*.[19] Elements to include in the framework are as follows:

**Strategic Vision.** To enhance the security of U.S. national interests, ensure the safety of the American people, and ensure that the United States continues to lead the world in the cyber domain.

**National Objectives (Ends)**

- Security, Prosperity, Values, International Order.
  - A safe, secure, and resilient cyberspace
  - Economic competitiveness
  - An open, interoperable, global Internet structure ("Shared, Connected Space)
  - A "rules-based international order"[20] that assures access and common behavior throughout shared spaces "as well as the dignity and human rights of all peoples"[21]

**Strategic Concepts (Ways)**

- Achieve NSS Interests by: protecting, projecting, partnering.
  - Protect constitutional rights including privacy
  - Protect intellectual property
  - Protect, enable, and sustain a free flow of goods, services, and ideas
  - Support innovation of individuals and businesses
  - Protect and support critical infrastructure
  - Share threat information as well as responsibility and management of cyberspace
  - Promote "global standards for cybersecurity"[22]

**National Power (Means)**

- Division of labor, education (public and private), establishment of norms.
  - Leverage all instruments of power to achieve ends
  - Establish cybersecurity maturity level and training standards
  - Establish incentives based programs for cybersecurity innovation and sharing of new techniques
  - Promote K-12 and higher education programs to develop future world class cyber experts
  - Establish a cyber small business innovation research program

- Maintain involvement and awareness of industry
- Hold exercises at every level of government (whole of community/nation participation)
- Assist in developing an international capability to investigate, deter, and disrupt cyberspace threats

**Outbrief**

On the final day of the workshop, members of the three breakout groups briefed a senior military representative from the NSC (Cyber Directorate) by teleconference on their findings while he reviewed the slides created by each group. A lengthy discussion followed (full transcription in Appendix B). Highlights included:

1. (NSC): "Why should there be a strategy for the Cyber Domain when the other domains don't have a specific strategy?"

   (GROUP): "This domain is unique in its pervasiveness, involving all elements of government, public, and international order. A strategy legitimizes the need for a 'whole of community, whole of nation' understanding of and preparedness for cyberspace threat."

   (GROUP): *"Seldom have we looked to the private sector for 'protecting' others (with the exception of safety) in a sense similar to military protection. With cyber being almost ubiquitous, even though it is an open-access domain, the other three domains don't really touch each and every person throughout each and every aspect of their lives throughout the day. How do you deal with the interconnectivity of things and technologies? It's not quite like the air and maritime domains."*

   (GROUP): *"Because it is such a new area, and because there are so many agencies and groups involved in it, we need to be working in one direction, pulling together; and we need something from a high level that coordinates our actions, including all the relevant agencies and industries, with everyone pulling in the same direction."*

   (GROUP): *"Other domains have quite mature and relatively stable treaty and legal frameworks in existence that deal with a lot of the contentious issues in those domains. Cyberspace is a domain that is not stable in the way we look at physical domains; it's actually morphing*

*all the time. If you don't have a more proactive and a more 'shaping' approach to this domain uniquely, then others will fill that space."*

(NSC): "*Are there any examples of a strategy document doing that across not just the whole of government, but industry as well? This is worthwhile, but also very ambitious."*

(GROUP): *"The new National Space-Weather Strategy is attempting to do some of that by bringing a 'whole of community' approach to something that impacts all the various infrastructures in a profound way, and cyber has that opportunity to impact infrastructure in many ways."*

2. (NSC): *"Wouldn't that be far more limited in terms of who would be participating?"*

   (GROUP): *"That depends – the new Space-Weather Strategy that just came out is going to result in an action plan that won't be articulated until probably September, but it calls for a 'whole of community' approach, every federal agency is supposed to be coordinated with a role. It includes state, local, territorial, and tribal governments and the private sector. They are asking each group to start planning for long-term regional and national power outages which basically is admitting that the impact could be very severe, and that somewhat similar to cyber, it could have an impact on industrial controls which could similarly result in long-term national blackouts with the potential risk of loss of sovereignty and severe stagnation or collapse of the economy. Those are the same kinds of things that we could be addressing or facing because of cybersecurity threats."*

3. (NSC): *"Do you envision some sort of regulatory or legislative initiatives to go along with the strategy, then – something to give it some teeth; or is it a lot of discussion about giving industry common goals to shoot for, having industry help one another with information sharing, etc.? I know there is legislation out there to do some of those things, but in many cases, industry is not interested in helping other portions of the industry because they are competitors. How would you envision this kind of partnering in authorship of this strategy? How would one go about doing that?"*

   (GROUP): *"The private sector group talked about that to some level of detail to include the question of…why would a competitor want to*

*help another competitor. When you talk about business and the core mission of an organization, that [helping competitors] becomes an issue, but not so much an issue associated with the protection of capability. …Industry is usually reticent to accept additional regulations; but sometimes, they do accept the need. In those cases, there needs to be a balance, and that is why industry needs to be involved in the discussion early-on. There are a number of different ways to do that. Some do it through consortia, some do it through other forums; but there has to be some lead that pulls everybody in."*

(GROUP): *"One of the things that resonated well with our group regarding the National Strategy for Information Sharing and Safeguarding was using the PPD-1 Process of Interagency Policy Committee and maybe with a subcommittee under the Cyber IPC, co-chaired plausibly by the cyber operations team, DHS, DoD, DOJ, using organizations like the Sector Coordinating Council, the Cross-Sector Cyber Security Coordination Group, and other elements like that, and of course, partnering with the Federal CIOs. Lots of existing organizations may find that they have a value proposition to seeing such a strategy get implemented. And also seeing the goals and objectives as not just guidance, if you will, or ideas from the administration, but a way (in line with these objectives for implementation) on how we can establish certain norms like we currently have in the maritime domain – the 'rules of the road' both nationally and internationally. The way we currently have the system of air traffic controllers – flight in and out of countries nowadays is almost normal [standardized]. But the truth of the matter is, having similar organizations come together to see that type of normalcy, at least from day-to-day operations in cyber, I think they would all find a value proposition and participate in putting together a national strategy for just that."*

4. (NSC): *"Do you view this as more of an inspirational document (e.g. this is how we feel as the U.S. Government and this is what we believe you should aim toward or strive to accomplish)? Or should this drive some sort of legislative strategy to actually put some teeth behind some of the initiatives here? Or if you are a holder of personal identifiable information that somehow gets stolen are you somehow liable for that?"*

(GROUP): *"Why not a combination?…Not just something that will be inspirational, but definitely something that would cause people to say 'if it's worthy of the United States to engage to the point of Executive Orders, putting fiduciary pieces behind it, grabbing their private sector entities and partners together, and leveraging their international partners to make this a normalcy for the world, it might be something unique – an opportunity to step out in the forefront.'"*

(GROUP): *"We had a lot of discussion about 'sticks and carrots' –they absolutely need to be part of this. Carrots could be incentives like tax breaks or insurance breaks.… This is an internal/domestic solution for defensive/cybersecurity measures. But for the external/international arena, we should be using all instruments of power to make sure that we are moving forward to what we feel are the correct norms and behavior in cyberspace, and making sure that there are consequences when people take actions in cyberspace that hurt us in one way or another."*

(GROUP): *"There is a category called 'coopertition' where industry players find it is actually better to collaborate on certain things while they are still competing on other things. There is also the adoption of best practices approach, where partners share packages of information that facilitate action, rather than having to take all the initiatives themselves. I think what we are looking at is a really multifaceted strategy that would engage a number of different types of interventions so that you wouldn't just be simply relying on what is a comparatively weak link in this, in that you could just pass a piece of congressional legislation*."

5. (NSC): "*I understand there are participants from private industry as part of your panels – what are your thoughts about the government somehow being able to mandate how they connect to the internet or how the handle their data? I'm sure that's bound to be controversial."*

   (GROUP): *"Critical infrastructure and Industrial targets (mostly owned by the private sector) are prime targets and highly vulnerable. Currently regulations leave them virtually blind, defenseless, and without a voice to describe threat issues as they experience them. Providing the public sector with access and the ability to participate with strategy and regulation development effectively decreases the country's vulnerabilities and increases national security."*

(GROUP): *"The private sector must be assured that cooperation doesn't further limit or degrade their ability to defend their own equities, and that their proprietary information is safeguarded by government entities. Any regulation would be looked at for its impacts, with respect to the way we already do business, the way we already connect, and what it would cost to implement. To the extent that it's something that is going to affect everybody, that's where we discussed thinking about means and ways to incentivize companies to do it earlier, rather than later.… This is about unfunded mandates, and the same thing happens on the federal side.…Somehow the means have to go along with the mandate, and certainly consideration with respect to what kind of a change accrues to companies [the consequences of implementation]."*

(GROUP): *"The National Strategy for Trusted Identities in Cyberspace actually speaks to [cost] efficiency and effective implementation.[23] The NIST framework was a result of that activity.[24] The voluntary way of implementing that, and some of the 'incentivizations' – and I loved the term previously used 'coopertition' – it definitely says (and companies do this too – some people want to wear that "badge of courage") – 'yes, I have fully implemented the NIST Cyber Security Framework; yes, I followed the internationally established cyber norms.' Often we've seen that when these things come out, if they resonate and there is a value proposition, folks are going to want to get in and buy in, even if it's not the right implementation timeframe and can be budgeted for or incentivized in some other way. We might find that folks are going to want to jump on, and not necessarily have to be told to get on."*

6. (NSC): *"I'm glad you brought up the NIST framework – that's where I was headed. In terms of offering incentives, there isn't a whole lot of spare capacity running around these days; but perhaps it's too early. We view the NIST framework certainly as being a 'positive' thing; but I don't know if it's had the 'branding' benefit that we'd hoped. Do you believe it's just a matter of waiting for that to occur or do we need to try something else?"*

   (GROUP): *"All of these things begin to merge, and go back and forth between these issues of what's the legal groundwork for our being able to act? What kind of playing field to we want to be able to have? Or do we look to government to sort out what is the information highway,*

*the information sea-lanes, the protection that we want as businesses to be able to operate not only within the country, but internationally.… When you develop standards [it] takes years vs. when you promulgate or encourage practices which might be able to move on a dime. There is probably a mix-and-match of those kinds of capabilities which allow businesses to move very quickly. Yet the businesses themselves…want the protection of government that would allow them to continue to exist. Some of these issues range from day-to-day little things that will eventually ding you to death if you are not careful, to existential threats and everything in-between. There is probably a range of frameworks between constitutional rights, the rights that are inalienably part of the citizenry, those that have to be part of the states, those that are part of the federal framework and international treaties. So it's a very complex mix. I think bringing the private sector in on an on-going basis to listen to their voices amongst others as to what we need to do to navigate through this would be important."*

7. (NSC): *"One of the documents initially referenced was the International Strategy for Cyberspace, 2011.*[25] *No doubt that is ready for a new look through the lens of the National Security Strategy; and I think that we've learned over the past four years – we've had destructive cyberattacks here at home, we've had an increase in capabilities of some threat actors, all of which I believe would be welcome additions to the already existing strategy."*

   (GROUP): *"We were hoping to leverage existing work.…There were some correlations between some of those strategies that we listed. For instance, the trusted identities piece – it talks to security, the openness, the cost effectiveness of doing cyber.*[26] *The National Strategy for Information Safeguarding spoke to the information piece as an asset, but it also looked at the infrastructure, foreign partners, private partners, state, local, tribal, territorial, all involved and engaged.*[27] *And of course, as you said, the International Strategy for Cyberspace speaks to that relationship. In one of our recommendations, we coalesce into a National Cyber Strategy, articulating even more clearly, or maybe even with a bit more resonance, that domestic piece and what it means to the international, and what all those things mean to those other communities of interest. So absolutely, this is not something that needs to be generated from scratch. It very much could be a matter*

*of saying that with the new 2015 National Cyber Security Strategy and what we've learned, maybe we don't need a separate strategy for the security and identity management piece, a separate strategy for the international piece, and a separate strategy for the information piece. It may very well be that there is a cyber strategy where all those things could now come together, merged refined and expanded upon and brought forward."*

(GROUP): *"What is interesting about the aforementioned strategies is that they don't reference each other. If you don't have them beside each other and do the crosswalk yourself, you can't see how they are tied to each other and how they broadly build, overlap and complement each other, which they do in a lot of different ways."*

(GROUP): *"What is lacking in current strategies is a coherent vision of how all elements of national power are supported and enabled by cyber. Cyber is covered, to an extent, by other strategies, but with emphasis on 'voluntary' compliance. Furthermore, the National Security Strategy mentions cyber, but only addresses 'ends,' vice 'ends, ways, and means.'"*[28]

(GROUP): *"Seeing that [existing strategies] are specifically oriented toward one of the interagency groups (DoD, DHS, DOJ, etc.), do you find (working at your level) that there are existing gaps and seams in terms of say tasking or authorities?"*

8. (NSC): *"Yes, we struggle with that all the time. Especially when it comes to authorities – there are different interpretations of that.…I would say, though, that there is some absolutely fantastic cooperation going on between Departments and Agencies, particularly in light of the OPM intrusions and all of the intrusions that we've had over the last six months. It's really driven the team together. We'll start to see this coming in the fall, when the Cyber Threat Intelligence Integration Center (CTIIC) will get rolled out. The intent of the CTIIC, as I understand it, is to take ownership of incidents and threat indicators in order to provide a multi-agency look at things. We'll have a number of embedded personnel from DoD, DHS, etc. working on the same analysis floor, to provide one source of information for not only the White House but other Departments and Agencies so they can all act*

*off the same sheet of music. So there are some ongoing efforts to try to get over those hurdles."*

## Conclusions

During the July 2014 Cyber Guard Exercise at Fort Meade, MD, USCYBERCOM Commander Admiral Michael Rogers stated: "Citizens of our nation are counting on us to generate the necessary capacity and capability to meet the challenges of this problem set." He conceded that meeting the challenges that cyberspace presents is very much a learning process for all involved: "We have to build a construct to work seamlessly and effectively with our partners, and not just within the government, but also with industry and academia – outside [the Defense Department]." The Cyber Guard event was reportedly a "holistic, whole-of-nation effort,"[29] yet a holistic, "whole-of-community, whole-of-nation" cyber strategy has yet to be articulated.

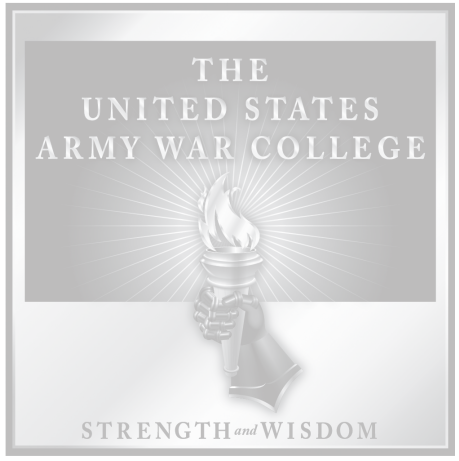
The requirement for a "whole-of-community, whole-of-nation" cyber strategy was verified during the June 23-25, 2015 Cyber Sovereignty Strategy Workshop. Although attendees discussed the concept of initiating a strategic document from scratch, the consensus was that there is much to be gained from building on existing sector/function/agency-specific cyber strategies, while using the 2015 *National Security Strategy* to anchor an expanded, comprehensive national cyber strategy.[30] As one group's briefer stated: "The desired (general) end-state is a cyberspace we can all operate in, from, and through freely with secure networks in peace, crisis, and war."

Private sector and allied/foreign partnerships, as well as the military services and government organizations (federal, state, local, and tribal) were determined to be vital to the process. The 2015 Cyber Guard Exercise – held from June 8-26 (which coincided with the Cyber Sovereignty Strategy Workshop) – reached the same conclusion,[31] stressing the value of partnerships between the military, government agencies, the private sector and allies.

Workshop participants sketched a very basic framework for a National Cyber Strategy over the 3-day period and welcomed the opportunity to converse with someone working cyber issues at the NSC level. The outbrief and discussion session was well received by the NSC

representative. He stated: "I appreciate the effort that you and the whole team put in on this. I think that there are seeds to some good and potentially powerful things here."

The NSC representative requested the opportunity to remain engaged with the USAWC on cyber issues, and offered to assist with the next event. The results of both the Policy and Strategy workshops will be reviewed during the third and final workshop in this series.


THE
UNITED STATES
ARMY WAR COLLEGE
STRENGTH and WISDOM

# Chapter 3: Theory and Operations

## General Overview

Workshop planners and attendees embarked on the third event in the series one year after the second, having wrestled with classification constraints that would limit open participation to some degree. Success ultimately depended on having a sufficient amount of open-source data from academic and industry sources to address both theory and operations.

Due to classification issues, new DoD regulations, and the length of time that had passed since the previous workshop, several attendees were new to this series; therefore, some strategy and policy material was presented as a series overview. This provided an opportunity to cover material published during the hiatus, as well as to showcase a few of the authors.

Pre-conference reading material included Lieutenant General Edward Cardon's 2016 article entitled "The Future of Army Maneuver Dominance in the Land and Cyber Domains,"[1] which presented a scenario of a "combined arms maneuver simultaneously across the land and cyberspace domains." LTG Cardon's article set the stage for further deliberations and discussion of the current state of cyber theory, operations, and the desired capabilities of a future cyber force.

## Objective

The objective for the third workshop was to focus on theory and operations using the "Strategic Design Lens"[2] to understand the environment, understand the problem, and develop an approach. During the workshop, participants were encouraged to discuss and propose a national "focus of efforts" to accomplish U.S. cyberspace goals.

Consideration of the adversarial viewpoint is an imperative, and may especially be so with regard to cyberspace operations. As noted within the previous two workshops, understanding intent is a huge challenge; however, it is crucial to the determination of appropriate response. Adversarial activities are increasingly sophisticated and potentially catastrophic. There are threat actors who consider themselves to be at war with the United States; and a U.S. failure to respond – especially in cyberspace – may have unintended consequences that include escalation. Determining an appropriate response may mean the difference between what some see as a simmering "cyber cold war"[3] and full-scale combined arms maneuvers that include cyber operations.

Questions for discussion:

- How do state and non-state actors impact U.S. Cyber Sovereignty?
- Is there a need for a comprehensive Cyberpower Theory that includes sovereignty issues?
- What does "Sovereignty in Cyberspace" mean?
- Should the U.S. drive towards more or less "Sovereignty in Cyberspace"?
- What are International and U.S. legal limitations on cyberspace operations with regard to sovereignty?
- Is it in the U.S. interest to enhance international cyber law and/or norms?
- Should U.S. cyber laws be enhanced and how?
- What approaches should we take moving forward?

U.S. cyberspace goals are identified in:

- *The U.S. International Strategy for Cyberspace:* "The cyberspace environment that we seek rewards innovation and empowers entrepreneurs; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. This cyberspace is defined by four key characteristics:
    a. Open to innovation

b. Interoperable the world over

c. Secure enough to earn people's trust

d. Reliable enough to support their work"[4]

- *DOD Cyber Strategy:* "The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas."[5]

The desired outcome for this event is a list of recommended areas where the United States should focus cyberspace efforts to achieve its goals.

**The Environment**

The DNI, in his 2016 Worldwide Threat Assessment of the U.S. Intelligence Community as presented to the Senate Armed Services Committee, listed Russia, China, Iran, and North Korea as the leading state cyber threat actors. Non-state actors were described as "terrorists" and "criminals" with Islamic State of Iraq and the Levant (ISIL) being the only group specifically mentioned.[6] Director Clapper's description of the activities associated with each entity was brief, but effective for the purpose of notifying the Senate Armed Services committee of the general threat level. The most striking associations made were:

- Russia – a "willingness to target critical infrastructure and conduct espionage operations," as well as "continuing preparation of the cyber environment for future contingencies"
- China – "continues to have success in cyber espionage against the U.S. Government, our allies, and U.S. companies"
- Iran – "used cyber espionage, propaganda, and attacks in 2015"
- North Korea – "capable and willing to launch disruptive or destructive cyberattacks to support its political objectives"
- Non-state Actors – "ISIL actors targeted and released sensitive information about U.S. military personnel in 2015 in an effort to spur 'lone-wolf' attacks"[7]

Timothy L. Thomas of the Foreign Military Studies Office was the perfect keynote speaker, as his published in-depth analyses of Russian and Chinese views on strategy and warfare are highly illuminating with regard to information warfare and cyber issues.[8] Kevin Coleman of

KCInsights, followed with his complementary assessment of current and potential capabilities and intent attributable to non-state cyber actors.

**Russia**

Although Russian and U.S. military and political leaders think of sovereignty in similar terms, there are aspects of Russian concepts of cyber sovereignty that are slightly different. According to Russian publications, there are three forms of sovereignty:

1. State (with regard to foreign affairs/foreign policy)
2. National (politics; self-determination of culture and character)
3. Popular (refers to the "cognitive processes of the population")[9]

The *Russian Military Encyclopedia* defines sovereignty as the supremacy of governmental authority within a country and its independence in international relations.[10] Russia's leadership is increasingly worried about digital or cyber sovereignty, as the Kremlin believes that nations are trying to impede on that sovereignty when possible. For example, as of January 1st, 2016 foreign investors cannot own more than 20 percent of a Russian media outlet. On May 25th, Security Council Secretary Nikolai Patushev noted that the Internet and other information technologies "are increasingly used in the process of destabilizing the state, for interference in their internal affairs, and for the undermining of national sovereignty."[11]

By controlling Russia's cyber sovereignty, the Kremlin can ensure that color revolutions will be neutered. This is important, because President Vladimir Putin sees enemies everywhere and only with control over information can he feel secure.

Information superiority is also a key element to be maintained for use in the initial period of war, specifically for the purpose of gaining advantage going into war. If one gains a cyber advantage, then it will be possible to gain the initiative in a conflict and counter enemy efforts to do the same. Media and internet control are necessary in order to control the population within the cognitive realm ("if they cannot control media, chaos will ensue"). System stability is to be sustained at

all costs while the ability to disorganize and destabilize the opponent is highly valued.

Russia considers that information consists of technical and human aspects. Cyber operations (cognitive and technical) are to be used to "destabilize states" and undermine an adversary's *national* sovereignty.[12] Information superiority could thus be considered a "first strike weapon."

According to previous information security doctrine (updates are believed to be under consideration) there are 3 major threat vectors (or "triad of threats"):

1. Critical information infrastructure;
2. The use of intelligence services to undermine sovereignty; and
3. Violations of privacy and computer crimes.[13]

A recent book entitled *The Red Web* by two Russian authors, quoted the Parliament Vice Speaker as saying "We should provide digital sovereignty for our country."[14] The current focus on sovereignty stems from anxiety over color revolutions (e.g. Ukraine's Orange Revolution and Georgia's Rose Revolution) which began with protests over freedom of speech, Internet freedom, etc.

*The Red Web* includes a template for Kremlin control of the media. It lists the use of repressive legislation, followed by undercover operations by "hacktivists and trolls" which prompt a crackdown on the media. Next, Roskomnadzor is granted the power to censor and filter the Internet, Kremlin-affiliated oligarchs take over media companies, specific manufacturer provide surveillance equipment, and Putin's paranoia of enemies everywhere ties these actions together. Thus, control of the media is a tool used to maintain cyber and media sovereignty.

In May of 2016, Andrei Krutskikh (Russian Special Representative of the President for International Information Security Cooperation and Foreign Ministry Ambassador at Large), while discussing an April meeting between Russia and the United States, noted the concern of both countries over the possibility of digital/cyber escalation, which Krutskikh hoped could be prevented. In fact, when another Russian cyber specialist was asked what worried the Kremlin, he placed "escalation models" at the top of his list, with the destruction of "civil infrastructures" a close second.

There are five issues associated with Russian conceptualizations of cyber operations and sovereignty:

1. Information warfare is divided into **"information technical"** and **"information psychological"** which can be similarly expressed in the cyber world by the concepts of digital sovereignty and cognitive sovereignty. Control over both is the desired objective. This is seen clearly in the Russian military definition of information warfare, which consists of:

    a. "conflict between two or more states in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures [technical]; and

    b. undermining political, economic, and social systems [psychological]; and carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government [psychological]."[15]

2. **Reflexive control** is a manipulative tactic that forms the question: "How do I make you do something for yourself that you are really doing for me?" This is actually part of the aforementioned definition of information warfare. After the description of the psychological aspect of information war the definition adds: "forcing a State to make decisions in the interests of their opponents."[16] It is thus part of their understanding of cyber/information war. *The Red Web* provided an example of reflexive control in the digital realm. The example noted a spear-phishing message disguised as instructions for protesters who were preparing to attend an anti-Putin rally. The attachment contained malware that placed a virus on the computers of those who opened the instructions.[17]

    The book *Information War*,[18] written by S. P. Rastorguev at the behest of the National Security Council of Russia, opened with a reflexive control example. The book concerns mathematical models for placing subliminal messages into an opponent's mind – a form of information warfare using the psychological realm.

    Another element of reflexive control was seen in use with regard to Ukraine, Kosovo, and Crimea. This element consists of thought

control utilizing analogies. Demonization of opponents by superimposing a visual reference of their adversaries with images that have historically negative connotations to the population they are trying to influence (referencing Ukrainian actions as those of Nazis, an analogy to Russia's opponent in World War II, modifying perceptions so that they are more positive toward the Russian government's actions) is one example.

Reflexive control is used to push enemies into "acting first" by virtue of intentional provocation – offering a pretext for response. If, for instance, a provocation is interpreted as an intent to launch a catastrophic "first strike," the target of provocation may decide there is only one response – to launch a preemptive attack, which might actually play into the hands of the provocateur and result in harsh international reactions against the provoked (victimized) nation.

3. **Media control** is used to gain information superiority over an opponent while protecting friendly sources from adversarial infiltration that is maintaining media sovereignty. It is seen as an absolute necessity for achieving dominance over the adversary early in a conflict, especially during the "initial period of war."

   Media control equates to regime stability. Russian government control over the media is legendary, and involves both internal and external propaganda (television, print media, product design, etc.). Internal propaganda is intended to mobilize the population on the government's behalf; external propaganda is used to influence other populations, but especially Russia's Diaspora living outside the country. The military has their own media mobilization program. Propaganda and displays of military might are used for influencing members of the military as well as the rest of the population.

   Russian leadership has most recently engaged in media control to persuade internal and external audiences of their legitimacy in "responding" to events in Ukraine. They use forms of "deception, deflection of responsibility, outright lies, and the creation of an alternative reality"[19] in their propaganda campaigns.

Deception includes the use of Internet trolls - people who are paid for by the Russian government to write negative (e.g. for NATO member countries) and positive (for Russia and surrogates) messages in online forums. Outright lies are often used, especially when questions are raised about Russian activities that could be considered creation of a "pretext" that would cause another nation to act first, similar to the use of reflexive control.

Putin is essentially using the media to "create his own reality" for both internal and external audiences. In response to Russia's internal problems, media control has consisted of conspiracy theories, warnings about the impact of color revolutions, and statements about Russia being surrounded and victimized by its adversaries (e.g. the United States, NATO). All of these actions are expressed as ways that the West is impinging on Russian sovereignty.

4. **System control and cyber espionage** go hand-in-hand within the Federal Security Service of the Russian Federation (FSB). The FSB has, since 1990, used a "special regime of reconnaissance methods" against its own people called "SORM" (System for Operative Investigative Activities) which provides for the mandated collection, analysis, and storage of all data that traverses Russian networks, to include message content. All Internet Service Providers must pay for and install FSB monitoring devices. Over the past several years, these devices have included the following sub-elements as SORM activities moved from one phase to another:

    a. SORM-1 (mobile and landline telephone)

    b. SORM-2 (internet traffic)

    c. SORM-3 (all media to include social networks, storing data for 3 years)

Cyber activities are not limited to the FSB. There are directorates for cyber activities within the Ministry of Internal Affairs (MVD), the Foreign Intelligence Service (SVR), and the Kremlin's Federal Protection Service (FSO). Each of these services is required to ensure the nation's cyber sovereignty.

Russian hackers are widely known for their abilities from distributed denial of service (DDOS) attacks and cyber espionage to malware insertion. It's hard to definitively delineate the difference between individual hackers and government-sponsored cyber operations, but operational types, characteristics, and targets can indicate intent.[20] Still, Russia's leadership routinely denies any connection (other than the possibility of benefiting from a "patriotic" citizenship) with hacking. Recently, of course, the United States formally charged the Russians with the hacking of the Democratic National Committee.

Perhaps Russia's most famous software group is the international cybersecurity software company of Eugene Kaspersky, which is headquartered in Moscow and advises the Ministry of Defense (MOD) and FSB. They also sell anti-virus software and publish research in China, as well as almost 30 other countries. Some nations, however, fear the use of Kaspersky's antivirus software. Ukraine in particular has refused to allow government organizations to use Kaspersky's products, although its use is allowed by Ukrainian citizens. In consideration of their own security, however, Russia is replacing all foreign-made operating systems with the domestically-developed Zarya Operating system. Further, everyone in Russia's parliament has been told to use only domestically made cyber products.

5. **Information or cyber deterrence** should be considered in the sovereignty discussion. It is mostly achieved by attempts to intimidate using reflexive control or intimidation, with the intent being to make other nations fear intruding on Russian cyberspace and therefore its cyber sovereignty, since there were responses to which Russia could resort. Recent examples include:

    a. The "leak" (on Russian television) of a "top secret" 100 megaton nuclear torpedo called Status-6 which is able to evade our detection systems, reach Los Angeles, and cause a tsunami[21] – this "leak" was intended to inform other nations that if they violated Russian sovereignty, there were responses available to which there was little or no response, as these torpedoes could evade detection

b. Recent cyberattacks on power plants in Ukraine which took out power to over 225,000 people and seemed uniquely designed to send a message[22]

c. Cyberattacks on radar systems at air control towers in Sweden,[23] and a submarine in the water off the coast of Stockholm[24]

d. Submarines and spy ships noted operating near undersea cables carrying global Internet communications[25]

e. The unusual parking (in the wrong orbit) and maneuvering (between two U.S. satellites) of the Russian military Luch Satellite "on multiple occasions" and for periods of several months[26]

f. The Russian potential to launch "killer satellites,"[27] and kamikaze UAVs[28]

Russia's General Staff has discussed using a concept known as "new-type" warfare. There was a specific diagram associated with the concept (no such graphic was ever offered for new-generation or hybrid warfare, both of which attracted much attention in the West). In fact, a scrub of open source data available to the Foreign Military Studies Office for over 1500 days since 2013 resulted in zero references to "New Generation Warfare." In 2015, however, Chekinov & Bogdanov, who gained fame for their development of the new-generation warfare concept, also began using new-type warfare. In the last two articles written by this pair, they did not use new-generation warfare, just new-type. The new-type warfare chart, which was found in the *Journal of the Academy of the General Staff* (see chart on next page) notes that propaganda, cyber attacks, and software effects all play a role in future conflicts.

- Note the use of "information psychological" in the "Set of Indirect Actions" above.
- The bullets (or bubbles) "Preparing Armed Opposition Detachments and Send Them to the Conflict Region" and "Covertly Deploying and Employing Special Operations Forces, Cyber Attacks and Software Effects, Conducting Reconnaissance and Subversive Acts on a Large Scale" seem to describe exactly what has been happening in Ukraine.


The MOD appears to have a plan in place to continue to develop cyber expertise among new recruits and officers. For example, the Defense Ministry has created 11 or so "science companies" within the military. These companies are composed of young officers and soldiers with electronic, information, or cyber competencies. They work side by side with older, more accomplished experts in the field. That way a new generation of experts is being created. Among the companies are those focused on the development of electronic warfare capabilities and cyber capabilities, and these companies are located in important locations such as the National Defense Management Center in Moscow.

Putin, of course, has made it no secret that to him the dissolution of the Soviet Union was the greatest geopolitical disaster of the century. He hopes to win back some of this lost territory if possible. His risk calculus is different than that of many Westerners as a result. Putin, for instance, did not go into Crimea as the result of a long-standing plan. He saw it as an opportunity that contained the following aspects: a weak/exhausted and monetarily stressed U.S. military; a German leadership that seemed to be on his side, total chaos in Kiev, and Russian forces (Black Sea Fleet) already in the area. In fact, in a recent *Foreign Affairs* article, Putin admitted as much, that he saw it as an opportunity to exploit.[29] Thus he will gamble with the sovereignty of other nations, and this must be remembered.

Regarding Syria, Mr. Thomas opined: "I don't know if we've ever before witnessed a regional actor (Iran), a local actor (Syria), a non-state actor (Hezbollah), a national actor (Russia with its planes, ships, special forces, and GRU), opposition groups, and U.S. planes all in the same area. Warfare in that area of the world is extremely complicated in its own way; it's almost a new form of war (not to be confused with the "New-Type of War")." That is, the changing nature and character of war is in need of continual study.

Both Russia and China, who have been cooperating in the broader area of cyberspace,[30] understand that *whoever sets the stage, gains a strategic advantage, or attains the initiative first, holds a winning hand for the initial period of cyber war*. The Chinese, for instance, talk about winning victory before the first battle. The way you do so, Beijing believes, is preparing the battlefield through reconnaissance, finding vulnerabilities, and planting malware – then if the decision is made to go into an initial period of war, you are prepared.

**China**

*Baike*, which is similar to China's version of Wikipedia, interestingly states that sovereignty is "a type of supreme, exclusive political authority that is put to use on an area, a people, or individuals.…a force and volition for maintaining independence and autonomy from the outside."

One article noted that the idea of cyber sovereignty contained three pivot points, with regard to intention, practicability, and concern:

- Intention: cyber sovereignty is a pivot point not only for safeguarding national security but also for securing public privacy (human rights)
- Practicability: cyber sovereignty is the pivot point of cyber governance between the multi-stakeholder model and the multilateral model, and China wants to combine both
- Concern: cyber sovereignty is the pivot point between state sovereignty and global cyber governance[31]

In December of 2015, Chinese President Xi Jinping noted the need for "respecting" the right to cyber sovereignty – that countries have "the right to choose how to develop and regulate their internet."[32]

Still, while President Xi seemed to indicate that other countries' cyber sovereignty should be respected, China's cyber operations against other nations do not appear to be held to that ethic. China's leadership is not necessarily concerned about the cyber sovereignty of other nations.

There is a "Cyberspace Administration of China," which was directed by Mr. Lu Wei who also happened to be the Deputy Chief of the Party's Propaganda Department. Mr. Lu gave a speech in 2013, within which he listed cyberspace sovereignty as the first of four aspects of China's cybersecurity platform. (The other three were the security of Internet information, privacy in cyberspace, and information technology.)

In December of 2015, China's *Xinhua News Service* printed an article "Why does cyber sovereignty matter?" It described the participation of President Xi Jinping at the Second World Internet Conference, and quoted him as saying: "Cyber Sovereignty dictates that no surveillance or hacking against any sovereign nation should be tolerated in cyberspace."[33] China's Ambassador Liu Xiaoming followed up Xi's comment at a May 2016 Cyber Forum in England with a proposal that the concept of "sovereign equality [as] enshrined in the UN Charter" should be applied to cyberspace.[34] Mr. Liu further noted:

- Individual countries can choose their own path of cyber development
- Each country can develop their own model of cyber regulation and internet related policies
- Each country has "the right to participate in international cyberspace governance on an equal footing"
- "Approaches inherited from the cold-war years and zero-sum games should be abandoned"
- "No country should interfere in others' international affairs, nor engage in cyber activities that undermine the national security of others" (sounds like the Russians verbiage)
- "An arms race in cyberspace or cyber warfare must be rejected"[35]

However, China appears well organized to interfere in the cyber sovereignty of other nations with its comprehensive reconnaissance effort in cyberspace. A Project 2049 Institute report on the People's Liberation Army (PLA) reconnaissance activities delineated a series of bureaus within the Third Department of the General Staff that carry out various missions. Each bureau has a different mission, some focused on specific nations, while others focus on operations (e.g. line-of-sight radio communications, encryption, computer network attack and defense, intelligence analysis, missile tracking, etc). It is worth noting that in some sense the PLA appears more worried about Russia than the United States, if just the number of bureaus studying these two nations are considered.[36]

A U.S. report by the Mandiant Corporation published units, military affiliations, and faces associated with China's cyber espionage activities,[37] putting to rest the thought that China was worried about the cyber sovereignty of others. It has interfered in other nation's cyber sovereignty on multiple occasions and that of its citizens as well. For example, cryptic comments from President Xi at the Central Internet Security Leading Group in April of 2016 encouraged government officials to surf the internet to discover what people discussed, and to take online criticism of the Chinese government seriously.[38] In effect, he was advocating interfering in the sovereignty of his own citizens.

China established its first non-profit cyber organization in March 2016 with the founding of The Cyber Security Association of China, directed by Fang Binxing, developer of the Great Firewall of China. The association's membership includes a variety of internet firms, cybersecurity organizations, and academic research institutions. As an international cooperative venture, ties to Russia have been noted;[39] but the stated goal "is to 'serve as a bridge' between the Chinese regime and the public, and to 'organize and mobilize forces in all aspects of society to participate in building China's cybersecurity'."[40]

China and the United States held cyber talks in May of 2016, following the April talks between the U.S. and Russia. Interestingly, while the U.S. representative was a State Department coordinator for cyber issues, the Chinese delegate was an Arms Control Director – an indicator of the Chinese perspective on cyber activities.

Like Russia's leadership, Chinese leaders have their own form of paranoia as seen in lessons and games developed for children and the public. Children play "spot the spy" some umbrellas sport a hotline number to call to report risks, and posters have been spotted with a cartoon story of a Chinese girl who was tricked into leaking state secrets. It is interesting that authoritarian leaders feel so insecure that they have to mobilize their society with stories of spies all around. This paranoia extends to their own civilian economists, as well as military officers in their dealings with external entities.[41]

China's cyber sovereignty approach appears to focus on a strategy of gaining an advantage over an opponent while denying them such advantage over China's cyber sovereignty. The point of strategy from the perspective of the 2007 book *Military Strategy* is to gain an advantage over an enemy. Chapter ten of this book focuses on cyber, and includes activities such as proactively performing sabotage on vital enemy systems, conducting offensive attacks, and decisively conducting a crucial battle with a "positive situation" [a.k.a. strategic advantage]. A "positive situation" can be obtained by discovering vulnerabilities early, using reconnaissance capabilities.

With regard to reconnaissance, General Dai Qingmin, the former head of the Cyber Operations Directorate of the General Staff, wrote nearly a decade ago that: "Computer network reconnaissance is the prerequisite for seizing victory in warfare. It helps to choose opportune moments, places, and measures for attack." It is important to "Focus on collecting technical parameters and specific properties of all categories of information weapon systems and electronic information products." With reconnaissance strategic advantage can be won and one can win victory before the first battle.

Harvesting parameters allows the Chinese to construct counters and perform reverse engineering, something they are very good at accomplishing, of those systems.

In writing a 2005 book entitled *Deciphering Information Security*, Shen Weigung, the father of Information Warfare in China, noted that "the issue of security is an issue of technology, but above all else it's one of strategy."[42] Friedrich Engels (1820-95) used to say "Technology determines tactics,"[43] but Shen seems to indicate that technology now

determines strategy. As but one example, a quantum communications satellite originally scheduled for launch in July 2016, was slightly delayed, and successfully launched on August 16th, 2016.[44] Does quantum technology determine not only strategy but also sovereignty? One appears embedded in the other (strategy and sovereignty) – they seem to go together. Strategic advantage can enable the protection of sovereignty.

Shen advocated starting cyber education with strategy in a course he taught – specifically "U.S. Military Strategy," "U.S. Operational Philosophy," and "The Basics of the Taiwan Situation," followed by the mundane aspects of algorithms and digital computing. A second course begins with "Fundamental Military Command," "Military Command Automation Systems," an "Outline of Information Warfare," "Information Operations Technology," and then languages and coding. The third in the series of courses Shen teaches gets into "Computer Virus Program Design and Application," "Preventing and Remedying Computer Viruses," a "Study of Hacker Attack Methods," and "Information Attack and Defense Tactics." The last course begins with "Information Warfare and the New Revolution in Military Affairs," but eventually gets into an "Introduction to U.S. and Taiwanese Social Systems," delving into social media to see how people might be influenced.

A 2007 book on strategy by authors Fan and Ma, defines strategy in the following terms:

- The strategic environment is "the important foundation upon which military strategy is dependent for its formulation…the arena upon which the strategic directors are dependent for displaying their talent in planning and skill in directing."
- Fan and Ma then state that "The relationship between the strategic environment and military strategy is a relationship between objective reality and subjective guidance. Properly understanding and analyzing the strategic environment is the prerequisite for properly formulating and implementing military strategy."[45]

That is, once analysts can correctly describe their objective reality, they can then subjectively begin developing ways to manipulate it. In 2013, a book of *Lectures on The Science of Information Operations*" included

a section on decision making, which noted that "all correct strategic decision making is the result of subjective understanding paired with objective reality."[46]

Mr. Thomas noted that China views its objective reality as one that is being encroached upon by others, especially China's cyberspace, and freedom of the press offers too much information to the public. Therefore subjective manipulation of objective reality resulted in the construction of the Great Firewall of China. The nation's leaders also push China's cyber sovereignty before international conferences and call for properly managing one's own cyber terrain, among other issues. On December 31, 2015, the establishment of a Strategic Support Force was officially announced, which, according to Peng Guangqian the Deputy Secretary General of the China National Security Forum, "will be in charge of information and intelligence collection, surveillance, electronic warfare, cyber attack and defense technology, and space management." Sputnik (Russian TV) talked about China's new recon force, calling them "unprecedented, highly capable and ambitious."[47]

What is the objective reality of cyber to a member of the PLA?

- Surrogates work.
- No hard/fast international rules and regulations
- Even with evidence, it is difficult to pin blame
- U.S. control of internet is "not in line with democracy"
- The anonymous character of the internet
- Weak security systems can be taken advantage of – "loot a burning house" (stratagem applied to their cyber)
- Packets of electrons can go undetected for long periods
- Stratagems work with packets of electrons (rustle the grass to startle the snake; kill with a borrowed sword, etc.)

When viewed from the perspective of objective reality, one can more clearly find an answer to the questions "why don't the Chinese stop their reconnaissance activities?" With no rules and regulations to stop them, and with the ability to use surrogates and mask their involvement, the question becomes "More relevantly, why would they stop?" They are getting away with the acquisition of state secrets at no or little cost to date.

A "stratagem is designed to mislead enemy processes of perception, thinking, emotion, and will" – in other words, control the enemy's analysis and intelligence processing. The Chinese have applied stratagems to packets of electrons and "play with them" in accordance with old stratagems. For example, "kill with a borrowed sword," would be a stratagem that ran packets of data/electrons from one country through another to attack a third.[48] One would then be able to kill with a borrowed sword.

One Chinese reference noted that a goal "is to put the stratagem developer in sync with the enemy's 'intelligence-judgment-decision' process and induce the enemy to make decisions as one would expect him to do" (similar to Russia's reflexive control theory).[49] Thus, the extent to which the Chinese are "in sync" with the U.S. intelligence cycle and aim to manipulate should be a point of great concern to U.S. analysts.

A 2010 Chinese book named *Information Confrontation* notes that China must move from unitary to complex systems of stratagems, while incorporating science and information devices (which could mean artificial intelligence). Applications of complex stratagems must be designed by a special agency, implying that China may actually have a cyber stratagem agency that would concentrate on finding ways to get into systems. An example of a complex stratagem might be: an attack on a site in the Eastern part of the U.S. designed to draw out CERT teams and "exhaust the enemy at the gate, attack him at your ease" while simultaneously saving their best viruses and cyber attackers to attack in the West of the United States by "making noise in the east to attack in the west."[50]

China has long considered the use of various stratagems and asymmetric methods to gain a strategic advantage in cyber activities. One of the earliest and well-known efforts was in the 1999 book *Unrestricted Warfare* by PLA Colonels Wang Xiangsui and Qiao Liang. They raised the idea of "cocktail wars" in that work.[51] Here they are not talking about "new concept weapons" (e.g. lasers, directed energy weapons), but rather "new concepts of weapons." For example, how do you put together pieces from 24 different methods of war (e.g. cyber preemption, network reconnaissance, high-tech deception, financial

market disruption, network deterrence, etc.) to come up with a cocktail mixture for a cyber campaign that would result in a strategic advantage? In 2008, General Dai wrote about the same concept, noting "It is necessary to paralyze an enemy's transport, telecom, and power systems in order to introduce deterrence."[52] Such campaigns seem destined to interfere in the cyber sovereignty of another nation.

An even more dangerous cocktail mixture would be one composed of simultaneous Russian and Chinese actions. Relations between Russia and China have improved over the past few years, with cyber agreements, cybersecurity issue sharing, and joint exercises. In May of 2015, Russia and China signed an International Information Security Agreement,[53] the wording of which is reminiscent of Russia's "information technical/information psychological" template, demonstrating that the two sides think somewhat alike. Definitions from the treaty include:

- "Information Area: The sphere of activity associated with information creation, transformation, transmission, utilization, and storage exerting an influence on, *inter alia*, individual and social consciousness, information infrastructure [defined as the aggregate of technical facilities and systems for information creation, etc.], and information proper"
- "Computer Attack: The deliberate use of software (software and hardware) tools to target information systems, information and telecommunications networks, electrical communications networks, and industrial process automated control systems carried out for the purposes of disrupting (halting) their operation and (or) breaching the security of the information being processed by them"[54]

Clearly the continued study of Russian and Chinese cyber issues must continue. As these nations develop joint efforts in the cyber field they may present Western nations with entirely new models of reconnaissance and infiltration.

With regard to the question of sovereignty in cyberspace, how do you look at cyber terrain? It's very different than geographic terrain. What is included? How do you map it? These questions could equally apply to the topic covered by the next speaker, Mr. Kevin Coleman, in his briefing about non-state actors who collectively go by the moniker "Anonymous."

## Anonymous and the Concept of Virtual States

Kevin Coleman introduced his presentation as one which should be seen through the lens of a non-academic, non-government, non-political, non-military technology strategist with 25 years in the business. Having started at Deloitte, Mr. Coleman later went to Computer Sciences Corporation, and then left to work on a start-up called Claremont Technology Group. After a merger, he left to join another start-up – Netscape – which grew at 65,000% in 4½ years.

In the mid-90s, when the Internet was becoming popular for public use, security wasn't built into anything. Silicon Valley views the technological terrain differently than Washington D.C. and the DoD; thus tensions have developed. A recent example was a highly publicized difference of opinion between Apple and the FBI.[55] Mr. Coleman noted that there is now a "giant rift" in Silicon Valley because of that interaction.

The entire digital domain is different than anything we've ever had before, and we are trying to force fit this domain into comfortable mental and physical models that we've used in the military, intelligence and business for decades. It doesn't work. This is different and we need to treat it differently.

The amount of dynamic change inherent within the domain is causing unprecedented problems. How do users (private, government or military) keep up with change when so many obstacles exist (regulations, policies, and procedures)?

What happens when military and government systems and processes fall behind technologically? Can you protect and defend the country? One of the most significant changes is the influence of entities distributed all over the world and their cyber power projection. Technologies are enabling "virtual states,"[56] which, by virtue of cyber sovereignty, can influence world affairs.

Technologies that are "hot" – with three to four times more impact than the Internet had in the late 90s – are influencing the way in which people are doing business in the world, as well as the way people interact with one another. These new technologies have created "digital sovereignty" – or what Anonymous (a non-state cyber actor) calls "cyber

sovereignty." In fact, Anonymous has declared cyber sovereignty! What does that mean?

What does a response to an attack by Anonymous look like? How do you project power in this domain? Since Anonymous is practically 100% digital and has no physical assets, where will you send bombers when Anonymous attacks? Who owns the response? Law Enforcement? Intelligence? The military? It's hard to find a definite line as to where criminal activity stops and military operation begins. Is it feasible that there is no legal, ethical, and/or judicial method of retaliation when Anonymous attacks? How many cases have the FBI brought against Anonymous compared to the number of incidents that Anonymous has caused?

Anonymous is made up of rarely (if ever) self-identified individuals who may or may not have any assets, but are "passionate" in their ideals. They have created a dissident/anarchic organization within the digital environment that we will have to deal with at some point. Furthermore, their loosely-knit organization may be at a point where they meet the qualifications of a virtual state.

An article from September of 2015, entitled "How to create a virtual country"[57] is an indication of things to come. Speaking in the context of what the author calls "disintermediation of governance," he (the author) contends that the tools of building a nation exist within the digital arena (e.g. crowdsourcing and cryptocurrencies), and since the digital world has no physical boundaries, entire virtual communities (virtual countries) can be formed made up of real persons "living" anywhere in the physical world. Of course, many questions have yet to be asked and concerns yet to be addressed, but is it possible that "citizenship" in these kinds of communities could become a new "norm?" That is exactly what some are expecting and preparing for.

In February of 2016, a "constitution" (which can be used as a template) for a virtual nation was created using BlockChain.[58] Bitnation, the "author" of the constitution, has developed services of governance that include marriage and birth certificates, identity management, land registry, and notary capabilities, as well as Bitcoin credit cards. The legality of these items is questionable at this point in time, especially considering Bitcoin, itself, has come under extensive scrutiny over

whether it is a currency or a commodity. While there is yet no definitive solution, there is a temporary compromise describing Bitcoin as both.[59]

Mr. Coleman published an earlier piece (2012) that defined this type of "amorphous socio-political entity" (a virtual state) as "a nebulous community of individuals that self-identify and share in common one or more social, political and/or ideological convictions, ideas or values. They act collectively to influence and bring about changes they deem appropriate or necessary."[60]

A virtual nation-state would require a form of money, citizens willing to labor, and assets – all in the digital realm; and for the first time in history, everything needed for a viable virtual nation-state, exists in the digital domain:

- The capability to create and enforce the governing parameters (Constitution) of the virtual nation
- The structure to operate in a highly distributed, continuously changing digital environment
- The infrastructure to operate, govern, maintain, and defend a virtual nation

Anonymous may, in fact, be closest to a virtual state than other candidates. They have rules. Members must not disclose their identity or the identity of other members, talk about the group, or attract attention.

An Anonymous core has taken steps to excommunicate those found to be inappropriate for the organization. The structure has thrived as members flaunt their capabilities and highly adaptive nature while traversing the digital environment. As a means of growth, Anonymous even created their own "Black Hat Academy," training others in their own brand of "hactivism."[61]

Furthermore, Anonymous has a proven record of projecting power and influencing decisions. They have existed as a group for some time (since 2003), and have managed to garner an amazing amount of publicity.

Anonymous recently moved their presence to the Dark Web for better security. What makes Anonymous a state is they have chosen, developed, and implemented their own form of governance and are starting to ignore (they may or may not try to influence) the governance attached

to the physical locations of their "citizens." Theoretically Anonymous could declare war on another nation-state, take down infrastructure, and possibly more.

On the other hand, Anonymous has already declared war on another group that claims to be a nation-state, and has a virtual presence – the Islamic State of Iraq and Syria (ISIS).[62] Earlier this year (2016), Anonymous declared war on Donald Trump[63] – an act that, regardless of any estimation of success, could be classified as foreign interference with a U.S. political campaign given a scenario where the concept of a "virtual nation-state" is internationally accepted. He's under Secret Service protection – do they have an obligation to defend him in cyberspace? What happens if Trump is elected? Would that be a declaration of war against a conventional, physical nation-state?

Would conventional nation-states ever be in a position to officially "recognize" virtual nations? And if so, once a physical nation state recognized one virtual state, would they then have to at least consider all others who requested recognition? If the United States ends up recognizing Bitnation constitutions and virtual states, what's to stop the U.S. Government from having to recognize terrorist groups operating from within the United States as virtual states? Workshop participants engaged in a significant discussion on this, one noting that the United Nations would consider a virtual state as "anti-sovereignty" and never recognize this type of entity. Another pointed out that the "citizenry" of a virtual state wouldn't necessarily care whether or not they were officially recognized. What matters to them is how they view themselves and how they operate given that perception.

Mr. Coleman commented that the concept of virtual nation-states doesn't appear to be a topic for research anywhere, but perhaps it should be. Are we seeing the private sector rising up against former structures of government? Could this be a solution for groups who are running from persecution and genocide? Maybe – on both counts.

The Internet/digital domain has grown to the point where no one person has a grasp as to what is going on. At any point in time there are hundreds of entities trying to create virtual models. "One thing is clear: virtual states represent the latest in the evolution of society in the connected

world and they have created yet another cybersecurity challenge."[64] What will the impact be?

This departure from a historical context of geographical boundaries to political, cultural, and communal entities will call into question models that have been in place for years! The global implications (current and future) of this new paradigm must be carefully considered:

- What happens when a virtual state's, nation's or country's sovereignty comes into conflict with the sovereignty of the United States?
- How could the United States pose sanctions against a Virtual State, Nation or Country?
- Other than cyberattacks, what weapons could the U.S. military leverage to combat a rogue virtual nation?
- Given the random structure and the wide distribution of virtual nation supporters/citizens/hackers as well as their use of compromised servers and other computer assets, how could the military retaliate?
- Given the wide distribution of virtual state, nation or country supporters, wouldn't any action taken against them have to be, by default, a conflict between a state and each individual member of the virtual entity?

In 2000, Richard Rosecrance a political scientist at UCLA wrote, "We are entering the Age of the Virtual State - when land and its products are no longer the primary source of power, when managing flows is more important than maintaining stockpiles, when service industries are the greatest source of wealth and expertise and creativity are the greatest natural resources." He went on to define a "virtual state" as one in which territory is no longer the prime focus of national identity.[65] When you look at how far we have come in socio-technological interactions since Rosecrance made that observation, it is easy to see how a virtual-state, nation, or country is on the horizon.

**Understanding the Problem**

Having been treated to an in-depth view of the perspectives of some of the state and non-state cyber actors that have been found in cyberspace, attention shifted to a discussion of ethical, theoretical and operational

aspects of the cyber problem. This segment of the workshop included a presentation on legal expression of cyber sovereignty and a report on the new Cybersecurity Act of 2015, as well as an overview of the update to the National Cyber Incident Response Plan.

A year has passed between the second workshop and this, the third and final in the series. New material concerning the concept of cyber sovereignty (policy and strategy) has been published during this period. To update and add to the information previously reviewed, refresh the memory of those who attended the first two workshops, and provide an introduction to those who are attending for the first time, speakers with fresh insight on these topics were asked to participate in this session. Thus, some of the information that follows will be reflective as well as instructive.

**Sovereignty**

Dr. Milton Mueller, of the Georgia Institute of Technology's School of Public Policy, was invited to discuss the concept of Cyber Sovereignty. He began by asking: Does Sovereignty in Cyberspace exist? Do we want it to exist?

In his admittedly "provocative" presentation, Dr. Mueller proffered that "sovereigntist principles would wreck the Internet." The Westphalian model is not only inappropriate, but neither U.S. national security nor global public interest are supported by a Westphalian approach to cyberspace. "There is a better way (the principle of 'freedom of action' in cyberspace)!"

Sovereignty in the western sense is not purely a political, legal or strategic concept but a combination thereof. It generally implies "supreme authority" within "territorially bounded" units in a way that keeps one government out of the business of another government.

Political scientists who tend to look at sovereignty with "a jaundiced eye" (Krasner is cited[66]) have delineated 4 different meanings:

1. International legal sovereignty, which involves mutual recognition by other states with formal juridical independence (you can be recognized as a government, yet have no control over your territory)

2. Westphalian sovereignty, which excludes external actors from the authority structures in a territory (e.g. colonial systems) and independent exclusivity of political institutions
3. Domestic sovereignty, which indicates the ability of public authorities to exercise effective control within their territory
4. Interdependence sovereignty, which includes the ability of public authorities to regulate the flow of information, ideas, goods, people, capital, etc., into and out of their borders (the most relevant to cyberspace)

Interdependence sovereignty – the question of having control over what comes in and out of a nation's borders – is where cyberspace has a problem. It is difficult, if not impossible, to have total control over information.

Krasner calls sovereignty "organized hypocrisy." In his view, sovereignty is invoked when it satisfies a specific agenda, and thus works to the benefit of a nation to claim it; but "people [leaders] invoke sovereignty when it's in their interest and ignore it when it's not."[67]

The Westphalian model is supposed to have come about in 1648 at the end of the Thirty Years War. The main goal of the Peace of Westphalia was to end religious wars spurred by the reformation. The agreements drawn up between the major players gave each sovereign (e.g. King, Prince, etc.) the right to decide religious affiliation for the territory over which the sovereign had authority, so defined territorial borders (not recognizable at the time) were necessary for implementation. But the division of Europe into recognizable nation-states didn't really occur until late in the 19th century, and a "somewhat" Westphalian "world order" wasn't fully operative (due to empires and colonialism) until after World War II. That was the point at which the U.S. entered into competition with the Soviet Union over who would retain power over the new nations created during the process of ending colonialism and the beginning of self-determination.

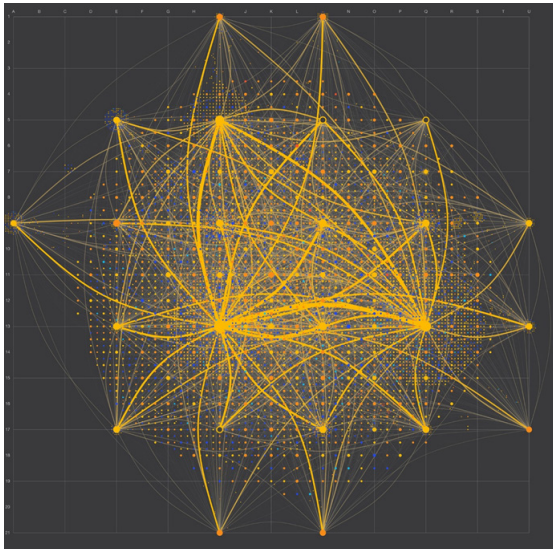
So do we want a Westphalian Internet? Interestingly, Russia, China, Saudi Arabia, Iran and France all like the idea of using a Westphalian approach to cyberspace. "Alignment" (the theme of this presentation),

is essentially "the attempt to cram global cyberspace into Westphalian boxes." Will it work? Is it a good thing?

There is a big debate going on right now in Internet governance circles – it's about "fragmentation," "balkanization," and "data sovereignty." This debate is really about making cyberspace mirror the fragmentation of territorial sovereignty on global scale, which the presentation called "alignment."

To fully understand alignment, you need to look at the postal, telephone, and telegraph ("PTT") monopolies of the early 20th century (the "apex of alignment"). These exclusive communications monopolies had territorial boundaries that "mirrored" that of the states they resided in.

As an incidental fact, the postal monopolies of Europe came into being around the time of the Peace of Westphalia. In other words, in order to establish a unified and territorially exclusive nation-state, they monopolized the postal infrastructure. Postal infrastructures, originally developed for horse-dependent transport, had high fixed costs and had to be maintained economically. Emerging nation-states began offering service to the public and charging for it as a means to support the postal systems that served as the backbone of territorial control. Eventually, competitors were banned (in Europe), and monopolies became the



**Map of Cyberspace**

norm, although competition in telegraphy and telephony did exist in the New World (the United States).

In Europe, PTT policies and priorities were set by the state, the communications systems were usually owned and operated by the state, and many of the larger nations had their own technical standards and "national champion" equipment manufacturers. This was the apex of alignment; but largely due to new technologies and the expansion of usage, countries have been moving away from this over the past 40 years.

Beginning with telecom liberalization, national markets and (subsequently) international markets began to open up to competition as privatization of the PTT monopolies became the norm. Deregulation ensued and trade agreements were negotiated, making competition for services and equipment even healthier. A new set of standards arose around computers and information technology that were, in effect, global in scope, but centered in the United States.

The Internet was therefore the last step in "smashing the alignment" of the PTT era. It was based on open, non-proprietary protocols and non-territorial name and number spaces (domain name system and IP addressing system). It is really a "software defined space" which depends on physical infrastructure but has its own distinct properties. There are logical and physical boundaries of the network, not based on political and/or legal jurisdictions. "Territory" is defined by blocks of IP addresses, but the process is about nodes and connections between nodes, not about geographic territory.

Is it possible to put the genie back in the bottle? Can we realign cyberspace and jurisdiction? Current attempts to do so can be seen in the nationalization of cybersecurity. Cybersecurity is for Internet users and providers. Most solution sets come from the private, as opposed to the government sector, yet cybersecurity is both a public and private "good."

There used to be transnational, loosely organized computer security Internet response teams, but these are now nationalized (e.g. the United States Computer Emergency Readiness Teams, or US-CERT[68]). With regard to the effect of information sharing on security, it may be the case that the insular nature of territorial fragmentation advances the case of cybersecurity – but fragmentation may also be hindering efforts to increase security.

The nationalization of cybersecurity has resulted in an increasingly intense interest in the origin of information technology goods and services. One example is the "banning" of Huawei, a Chinese telecommunications agency, from competing on government contracts.[69] A commonly cited concern is the association of developers with the military services of the nation-state from whence the technology comes. In reality, the fact that a developer in China had been associated with the PLA may be no more threatening than the fact that U.S. military service members may end up working for a major Internet provider in the United States.

Another effort to realign cyberspace according to territorial jurisdictions involves the territorialization of information flows (e.g. data localization efforts, the "great firewall of China," etc.). Data localization is a regulatory maneuver designed to keep data storage within territorial boundaries for the purposes of legal access. It's also a means of cybersecurity, in that adversarial nations could claim "ownership" of and a legal right to access data stored within their territorial boundaries (e.g. data localization keeps adversaries from claiming a legal right to data stored within U.S. territory). "It's about jurisdictional control. It's about alignment."

The third area where there are attempts to align jurisdiction and cyberspace is in critical internet resources (domain name and IP address standards and resources). In this sense, the "globalizers" have the advantage, as the internet's name and number spaces were designed with and developed global aspects.

One interesting attempt at alignment was seen when two Chinese engineers introduced a standard in the Internet Engineering Task Force (IETF) called "Autonomous Internet" – a proposal to restructure the Domain Name system. They suggested that every country should have their own "root" as a matter of sovereignty (the root is the highest level of the domain name hierarchy which is currently global and administered by the Internet Corporation of Assigned Names and Numbers [ICANN][70]). This would cause enormous disruption and create obstacles for global entities, essentially requiring the equivalent of the phone system's country codes (mirroring the Westphalian PTT model).

Although this proposal would never be accepted by the IETF or the global Internet service providers, it provides a good example of how the

sovereignty model would be applied to the domain space. It would be very hard to undo the numbers and addresses that have already been allocated in blocks around the world. Still, there have been attempts by authorities to somehow input data into the number registration database that links things to jurisdiction. Law enforcement authorities are pushing for this – for perfectly legitimate reasons – but their mindset remains Westphalian, thus they don't quite understand the implications of what they are proposing. Network nodes may be in several different countries, with users located around the globe, thus jurisdictional access is difficult to enforce.

Given all of the above, what does sovereignty in cyberspace mean? It means:

- Alignment of the autonomous system and jurisdiction
- Alignment of Internet virtual resource assignment with jurisdiction (which would include AS Numbers, IP addresses, and domain names)
- National chokepoints for online service provision (for content filtering, blocking, etc.)
- National certification of end user devices and infrastructure equipment if not a return to the old model of a national provider or supplier
- National certification of software applications (no more ad-hoc creation of applications, games, etc.)
- The ability to detect and verify movement and location of all data (harder than it sounds, due to multiple copies, massive numbers of resends, etc.)

Therefore, based on this list, sovereignty may not be such a good idea in cyberspace.

The structure of the Internet is very globalized, and the structure of sovereignty is very territorial, and it's very hard to reconcile the two. Furthermore, sovereignty has no bearing on or any relationship to what people actually do in a military or national security sense.

What is a non-territorial approach? Freedom of action in cyberspace! General Alexander, in a statement before the House Armed Services Committee said that the U.S. strategic objective is to "ensure U.S.

and Allied freedom of action in cyberspace, and deny the same to our adversaries."[71] The concept, as stated in JP 3-0: *Joint Operations* (August 11, 2011),[72] is (as noted by Dr. Mueller) an equally narrow, military-operational definition of "freedom of action."

The idea of "freedom of action" is interestingly undeveloped in cyberspace, and we need to think carefully and more extensively about the concept. It's actually the right approach, but a broader, politico-economic definition may be more desirable.

The United States has traditionally fought for freedom of action in oceans and outer space. Freedom of action as it applies to the oceans is older than the Westphalian model:

- In 1609, Grotius articulated the principle of Mare Liberum (Freedom of the Seas)
- In the 1780s, early American political leaders (Adams, Franklin) championed the view that the seas ought to be free in war as well as in peace
- In 1917, President Wilson asserted the right of every nation to have free access to "the open paths of the world's commerce"
- In 1941, the Atlantic Charter set forth the affirmation that "peace should enable all men to traverse the high seas and oceans without hindrance"

There have been contradictions and deviations from this principal, such as conflicts and issues concerning the rights of neutrals during a war, as well as the rights of belligerents to blockade the seas. Although there have been exceptions, the United States has, in general, been consistent about keeping the seas open to commerce, and maintaining freedom of action in the seas for the world. There is serious debate as to how far this goes, as instances of creeping territorialization of the ocean (attempts to extend sovereignty beyond agreements) increase in number, and exclusive economic zones grow larger.

Freedom of action in outer space is even more interesting. Before Sputnik, the United States was very much in favor of the idea of space as a global commons. Surveillance was a concern at the time, but space has since developed into a place where both military and civilian activities are vital and intertwined. Regardless, important distinctions

are made between military *uses* of space and the *weaponization* of space objects.

In order to keep the militarization of cyberspace from undermining its value to the civilian economy, freedom of action in cyberspace might take the form of:

- Respect for every lawful actor, not just the U.S. military
- Not unilateral dominance but a recognition of the public benefits of open global communication, closely tied to the principle of freedom of commerce, free expression, etc. (the United States has most to gain from a global Internet as well as the most to lose from its disruption)
- Justification of extensive, global situational awareness within the limits of the Constitution
- Justification of the use of cyber force, and possibly kinetic force, against those who would abuse their freedom of action in cyberspace to threaten U.S. national security, regardless of where they are located (realizing that retaliatory actions and deterrence effects are difficult to limit to U.S. territory, or even U.S. citizens)

How deterrence works and how retaliatory actions occur in this type of environment is open to debate – and indeed, debate ensued. Discussion centered on the fact that individuals cannot legally "attack back" following an attack against their systems. Individuals are allowed to "defend" only by virtue of having cybersecurity resident on their systems (anti-virus software, firewalls, etc.); yet there is no means for individuals to report attacks on a timely basis and get assurance of a response. Questions were raised about the lack of legal action taken against U.S. companies who may use such techniques in order to respond to cyber threats. Where is the line between self-defense and offensive action?

Will there be some global jurisdictional body set up to establish what is appropriate, and what isn't – something like the International Criminal Court? That may be difficult in this environment, especially with regard to countries who would disagree with the U.S. perception of freedom of cyberspace. Dr. Mueller doesn't see an International Court as a necessity – but if one was to be emplaced, it would have to be

defined within the framework of the International Laws of War (norms that states can follow or disregard based on their own interests). Dr. Mueller admitted that he is actually assuming anarchy as opposed to an ability to garner "hard and fast" agreements.

Still, a participant noted that what is going on right now is a process of nations deciding who the jurisdictional authorities are. Going global establishes a requirement for a global body that regulates. Who will make the decision on whether certain activities would be considered espionage, and whether espionage is allowed? Espionage is defined by different nations in different ways, and there is no current jurisdictional baseline that says "it is" or "it isn't." The participant claimed that there must be an organized body that regulates these issues, leads in development of agreements, and it can't be the market because the broader decisions can't be left to individual companies.

Does it have to be global? Most of the current agreements are in the private sector. The United States doesn't want cyber treaties, or global regulatory bodies; but it does promote norms of conduct, and is already encouraging a multi-stakeholder process with minimal regulation. We have created a global organization called ICANN and we have just decided to "destate it." We have decided to "desovereigntize it" by pulling the U.S. Government away from its special authority over it, which "was a big sore point with the rest of the world," making into a pure multi-stakeholder, private sector-based organization.[73]

A question arose concerning major/catastrophic instances of conflict across the globe, with a need for unity in evidential discovery and response. What would everyone need to agree to in order to make this kind of response possible? Would such a response change the role of government involvement, even if everything was loosely regulated and market driven leading up to the event? Dr. Mueller cited Louis Pauly, a political scientist in Toronto, who had previously asked him a similar question. One of the theories of sovereignty is "he who decides on the exception."[74]

Who has enough authority to act, stepping outside all of the rules, if there is some kind of a crisis? What is the ultimate authority for coordinating a global response to a cataclysmic event? Based on

the answer to that question, specifics for political cooperation and institutions will begin to form.

The concept of sovereignty is very fluid historically. When there is an external threat, new forms of political institutions will rise to the occasion; but it would be foolish to try to predict how any scenario would play out. It would be very wise, however, to consider how political structures would handle a catastrophic event while avoiding other major problems, such as a global uprising or major meltdown of democratic institutions.

**Theory**

Dr. Jan Kallberg from the Army Cyber Institute at West Point joined us to discuss Strategic Cyberwar Theory, as reflected in his recent article published within *The Cyber Defense Review*. Dr. Kallberg used "Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations" to propose a framework which he believed would "change the way nations view cyber."[75]

Dr. Kallberg began the discussion with a quote:

> *Cyber is now recognized as an operational domain, but the theory that should explain it strategically is, for the most part, missing. It is one thing to know how to digitize; it is quite another to understand what digitization means strategically. The author maintains that, although the technical and tactical literature on cyber is abundant, strategic theoretical treatment is poor.*[76]

Can we have much impact on future cyber conflicts? Is leading cyber (with regard to commands, leadership decision-making, etc.) an illusion? Are we products of our past in the way that we are conditioned to lead? When operations reach machine speed, commands may have to be "pre-given instructions."

With cyber, maybe we are dealing with a completely different functional concept, needing a different strategy. The enemy used to "'behave' – a good leader could size them up. This is no longer the case.

The four tenets of cyber are: Object Permanence, Measurements of Effectiveness, Machine Speed in Execution, and Anonymity.

There is a physical layer, but do we have "object permanence?" If not, maybe traditional military thinking doesn't work. In Clausewitz's time for instance, geographic characteristics within the environment didn't change overnight. In cyberspace, the environment changes at machine-speed.

Measurements of effectiveness used to be relatively easy to come by. Numbers of personnel remaining in battle, numbers of weapons and weapons systems, could all be garnered through intelligence, if not by other means. In the digital arena, measures of effectiveness are difficult to determine – especially since the opponent continues to "stand." A leader can no longer tell what's happening on the other – the adversary's – side. Cyber battles can be waged with opponents thousands of miles away. Furthermore, things may be going on within a leader's systems that remain unchecked until it's too late. Regardless, the fact that the targeted "weapons systems" are the same systems that harbor necessary intelligence data, poses a unique challenge to leaders who must make decisions with regard to battle damage.

Machine speed in execution is virtually impossible for humans to carry out, and when considering the layers of bureaucracy through which decisions are made, cyber systems are impossible to compete with. Also, the anonymity that can be achieved via the use of hacked or surrogate systems, makes it difficult to survive an initial onslaught in a cyberwar. For premeditated attacks, there can be long (days, months, years) information gathering cycle in preparation for execution, which may last only a moment in time.

Cyberspace operations shouldn't be seen as just another joint force enabler. There is a reversed asymmetry that must be understood – a state can attack a domestic public entity as well as individual citizens, and vice versa. Cyber conflicts of the future will not simply be a match between military networks, and leaders must not fall prey to the belief that we will always have a counterpart in cyber conflict that buys into our normative concepts.

Our leaders will fail if they continue to rely on non-existent measures of effectiveness (MOE). They will fail if they continue to resist the acceptance of the rapid timeframe in which interchanges will occur – if they do not comprehend the consequences of automated harvesting of vulnerabilities and execution of attacks at computational speed. They

will fail if they do not factor in the impact of artificial intelligence used in combination with a multitude of system exploits.

There is a great deal of increased spending on cyber activities, but with no thought as to a desired end state. Consideration must be given to effects. We assume that when critical infrastructure goes down, people will be upset, there will be turmoil, a disintegration of society; but on the positive side we know that when the Germans bombed London, it only hardened the British. When the war started, many of Churchill's cabinet were in favor of appeasement with Germany. After the bombs began to fall, British unity showed up in full force.

People may not act the way we assume when critical infrastructure is taken down. When the most recent major blackout in New York occurred, many were more cordial than they would be during a normal workday. Thus, it may not be the case that if the United States is "hit" with a cyber attack, it will have a devastating effect on society. Much will depend on the government's relationship with the population and how much trust people have in the government. (As workshop participants pointed out, this is assuming a short-term, easily mitigated attack with few actual consequences. A plethora of studies have verified that a long-term [months to years], critical infrastructure outage will indeed have devastating, if not catastrophic consequences to the population.)[77]

Institutions matter in societies. If you have strong institutions, you might not be prey – you might be predator in a future cyberwar. Using Bertrand Russell's version of Occam's Razor – "Whenever possible, substitute constructions out of known entities for inferences to unknown entities."[78]

Dr. Kallberg developed his own Strategic Cyberwar Theory: "The utility of cyber in an offensive strategic role is determined by the institutional stability of the targeted nation."

- To gain a strategic cyber advantage that will lead to the adversary's submission to foreign power, the magnitude of the operation has to impact the targeted society's stability – a "blunt force" initiative. You must "hit them with a blunt hammer." Otherwise, it's just noise.
- Institutional frameworks are the foundation for any society as these institutions forms the glue that holds the society together.

- Systematic attacks on institutions, coming from different angles, can destabilize a society.
- The currently limited and unsystematic forms of cyberattacks will not trigger strategic advantages.
- Time is of the essence, especially considering automated premeditated attacks. There will be little, if any, time for response.

Dwight Waldo, a mid-20th century political scientist and author of *The Enterprise of Public Administration*, described a legitimate regime as one with the ability to provide citizens with a "good" life. The regime must have the authority (internal and external) to implement policy and decisions and the control to ensure implementation. It must be a functional institution of knowledge in government, and must maintain the confidence of the population.[79]

Using Waldo's five factors of legitimate regimes, a target matrix can be developed:

| TARGETING MATRIX EXAMPLE | |
|---|---|
| **Waldo's Five Factors** | Example of Targets |
| **Legitimacy** | Legislature<br>Welfare Benefits<br>Classified Information<br>"Leaks" |
| **Authority** | Law Enforcement<br>Local Government |
| **Institutional Knowledge** | Cadastral Data<br>Tax Collection |
| **Control** | Air-Traffic Control<br>Railways<br>Payroll |
| **Confidence** | Energy Providers<br>Retirement Funds<br>Public Financial Support Transfers |

**Table 1**

Dr. Kallberg encouraged participants to "flip that" – what makes an "awful" society? A study of institutional patterns indicates that some countries correlate, some do not; but institutional differences can create cyber vulnerabilities. By targeting these vulnerabilities, you can destabilize a society.

- If cyberattacks are unsystematic and with limited ability to destabilize it is like rain on a parking garage;
- The pressure from these attacks is distributed evenly over the institutional framework that upholds the society; so
- Dr. Kallberg's Strategic Cyberwar Theory seeks to identify the framework that upholds society – and remove critical pillars to trigger a destabilization utilizing the dormant entropy in society.

The operation plan for these targets should consider the following:

- To trigger popular unrest, financial chaos, or societal destabilization the attack must be concentrated in time
- The targeted points must have the potential to break up institutional stability – each society is unique
- A quick conflict avoids triggering an adaptive behavior in the targeted society
- Focus on what matters for the vocal population instead of what matters to the defense establishment
- Government entities, by default, see themselves as influential and capable, but in the short timeframe a cyber conflict is fought, the reach of government can be limited or non-viable
- Concentrating solely on a military perspective will create a bias toward military or defense industry information assets

Traditional sources of authorities are no longer there as governments and societies move online. There has been a corresponding change in people's relationship to government. Thus, several of our potential adversaries have dormant empathy – an underlying instability that is already there. Cyber operations must therefore involve seeking out weak spots and trying to exploit them. If an attack doesn't significantly harm the targeted regime, it is merely noise.

- Several potential adversaries have dormant entropy by virtue of the design of their regime and suppression of the population
- If it doesn't hurt the targeted regime – it's noise – that's why a systematic destabilization attack is a real tangible threat
- Quick execution creates system shock and loss of control
- Limited random digital exploits are a cyber annoyance – not war

What if government is not there? China, Russia, Iran, and North Korea are countries on the brink of negative entropy. They have weak institutions and put a lot of resources into controlling their societies. The result of destabilization could be devastating.

For cyber defense we must identify institutions that have an impact on our societal stability and provide support to them, if necessary. Public and private entities must approach cyber defense unburdened by traditional thinking (cyber defense is not only information assurance). In so doing, we must seek to embrace the future detached from the earlier cyber funding paradigm.

Small events can have big effects. Cyberattacks can influence social stability if it strikes the right cord. The good news is that if the utility of offensive strategic cyber is dependent on the institutional arrangements in the targeted society, the United States and allies are predators and not prey. The fact that we have stable societies means that at critical junctures our population won't take to the streets and do bad things.

The United States is in a strong position because our society have resilient and strong institutions – this is the strength of democracy. Open government and transparency strengthen societal resiliency. Although open government increases the potential target area, higher resiliency provides a balancing element.

You can embed cyber in many ways as an enabler in support of battlefield objectives; but if you're just going to use cyber for decisive action, how are you going to do it? What matters in society? What can we not allow to go down?

As stated earlier, institutions matter. Failing institutions will negatively impact society through entropy that unleashes dormant challenges to governments in targeted countries. Additionally, rapid execution

and "blunt force" is needed on an initial strike – otherwise adaptive behavior and tit-for-tat will follow, with no decisive outcome.

A participant asked whether consideration was given to the possibility of there being a threshold at some point lower than total loss/collapse where the U.S. Government would acquiesce. Dr. Kallberg responded with his own belief that in a degraded environment, we trust our law enforcement and are usually orderly, which, to him, shows a piece that is missing in the current cyber discussion – that the United States has a built-in resilience which we (and our adversaries) might underestimate, even under a "Cyber Pearl Harbor" scenario.

This brought about a discussion of scope, level, and duration with regard to determination of existential threat. At what point does the social fabric start to break down, and the social structures that maintain societal resilience begin to disintegrate? Dr. Kallberg suggested that the point is probably close to where health becomes affected.

Another participant raised the point that countries with less developed institutional stability are also less developed technology, and are thus less susceptible to cyberattack. Dr. Kallberg additionally noted that information denial can induce a certain amount of paranoia among both the population and government, resulting in a restrained use of internet communications. It was generally agreed, however, that there would be a "set of thresholds" at which tolerance is no longer acceptable. It will be a political decision with regard to legal authorities as to whether there was an attack on the homeland, and the equivalency of that attack (or not) to an "act of war."

Dr. Kallberg concluded by asserting that the vast majority of services that people really care about are provided by counties, towns, municipalities, etc., and (to a degree) states. In his opinion, we don't put enough emphasis, with regard to the cyber discussion, on counties and municipalities. There is a great need for a national survey as to what institutions and services matter most to people. Are we doing enough to protect our own institutions? We don't really know at this point.

**Sovereignty, International Law and Cyber Deterrence**

Colonel Gary Corn of USCYBERCOM, graciously offered to update attendees on relevant international law and describe its relevance to

sovereignty and cyber deterrence from the perspective of military planning and operations. He explained that currently there is uncertainty among experts, both within the United States and internationally, over the exact meaning of sovereignty in international law and its applicability in cyberspace – specifically whether the unauthorized access of computers or networks located in another country violates territorial sovereignty and/or international law.

With respect to cyberspace, some have questioned whether law even applies. Is cyber so different that law doesn't apply? No – law matters and the consensus among international experts and States is that international law applies to cyberspace and cyber operations. But there are questions as to exactly how it matters in cyberspace. Within international law, what does the concept of sovereignty mean and when is it relevant to cyberspace? What does international law have to say about cyber deterrence? How does it impact planning and strategy development – feasible, acceptable, suitable strategies to implement in the cyber context?

As background, COL Corn discussed a recent decision of the International Court of Justice (ICJ) involving a heavily disputed area between Nicaragua and Costa Rica. The ICJ issued a ruling in December of 2015 on this disputed area. The bottom line – Nicaragua had a perception of where its territory was, and began to dredge canals on that territory to open up waterways. While doing so, it moved military troops onto the disputed territory. Costa Rica asserted possession of the territory and claimed that Nicaragua's acts constituted a violation of its territorial sovereignty and hence international law. Nicaragua denied the claim, and countered that Costa Rica had carried out some road development that caused sediment to shift down into Nicaragua's territory, thus violating its territorial sovereignty.

After first resolving the territorial dispute in favor of Costa Rica, the ICJ then found that although Nicaragua's actions "did not constitute hostile acts" as defined in an 1858 treaty between Costa Rica and Nicaragua, and thus did not rise to the level of a prohibited use of force in violation of Article 2(4) of the United Nations Charter, they nevertheless were a breach of Costa Rica's territorial sovereignty subjecting Nicaragua to the obligation to pay reparations for the damage caused by its unlawful

activities. The court then rejected Nicaragua's counterclaim that the sediment constituted some form of invasion or violation of sovereignty.

Why bring this up in a cyber workshop? Because some point to the ICJ's finding that Nicaragua violated Costa Rica's "territorial sovereignty" as evidence that international law prohibits the entering into the territory of another state without consent, at least where there are some impacts therein. There is ongoing debate among some in the international law community – specifically those working on the next Tallinn Manual – over the correctness and contours of this assertion.

Some take a very strict view of sovereignty. They see it as almost an international rule of trespass. So if there is any non-consensual entrance into the territory of another state you have breached an obligation, you have violated a rule of international law.

If you respect the rule of law, if you tend to want to conform your conduct as a state to international law, that's pretty significant. Others, including COL Corn, interpret sovereignty – to include the concept of territorial sovereignty – as a foundational principle of the international system underlying specific rules of international law, but not a rule in and of itself. Those who espouse this view assert that one must look to the UN Charters prohibition against the use of force, or the customary international law principle of non-intervention, to assess the legality of states' actions in cyberspace.

Discussions about this have been raised in the context of espionage. States have conducted espionage since time immemorial – certainly since Westphalia. Espionage frequently involves entering into the territory of another state without consent or under false pretenses. Most states (to include the United States) have legislation and policies that acknowledge this. Thus, there is inconsistency – doesn't that make espionage a violation?

Most experts agree that international law does not prohibit espionage. It may be criminalized by the state in or against which it is conducted, but that's a different question. It is not prohibited by international law.

If one adopts the trespass theory of sovereignty, then the fallback is to claim that there is a long-standing carve-out in international law specific to espionage, based on state practice. States have been doing it

for so long, that we accept non-consensual incursions in this narrow area of espionage.

Regarding cyber operations more broadly, however, the coin of the realm is access – preferably persistent, stealthy access. Gaining unauthorized access into the computers or networks of a target or third-party state without consent may not be for espionage purposes, especially in a deterrence framework, and thus implicates directly the question of the exact meaning and import of territorial sovereignty in international law.

Like the Computer Fraud and Abuse Act in the United States, many states have statutes on the books criminalizing unauthorized access to computers or systems. If you are gaining access to someone's computer or system without authorization, or exceeding the authorization that you have to be there, you are in violation of federal law. However, that's a matter of domestic, not international law, unless a strict trespass rule is upheld as such.

How does sovereignty play a role in this issue? Some take the position that cyberspace is such a new and unique thing, that there is no sovereignty in cyberspace. Sovereignty is an irrelevant concept to cyberspace. Others recognize the foundational importance of sovereignty, to include its applicability to cyberspace, but differ on the narrower question of how international law applies to and regulates activities in cyberspace.

Irrespective of the ICJ's specific holding regarding the positioning of military forces, dredging, etc., on disputed territory in Central America, it is the position of the United States, along with a majority of experts, that based on sovereignty states can exercise jurisdictional rights over the physical cyber infrastructure and can proscribe the conduct of individuals in cyberspace that reside within their territorial boundaries. The very fact that the United States has a Computer Fraud and Abuse Act tells us that there is a sovereign right to regulate some cyber activity.

As noted earlier, the law can be argued in terms of an "espionage exception" effected through cyber means; but that doesn't necessarily work if the issue is about conducting other operations through cyberspace. When you talk about a deterrence framework – the ability to hold targets at risk and having the accesses you might need to do

that, especially if you are in a state of peace, trying to prevent war – how does that work with this concept of sovereignty?

Jean Boudin (1530-1596) was a lawyer credited with laying the foundation for the notion of sovereignty that later developed into what is seen as the beginning of the nation-state period. He is credited with the concept of the absolutism of sovereign power – that within the sovereign's realm of territory, he or she is not bound by the laws, but is the giver of laws. The sovereign is supreme within his or her space. The sovereign exercises absolute power and control within his or her territory.

Thomas Hobbs (1588-1679) wrote the book *Leviathan* as an analogy to the state, where we cede over all of our power to the sovereign. Hobbs took this notion of internal sovereignty and the control that the state has within its own territory, and followed on with an absolutist view, looking externally. What is the relationship of states between each other? And how does sovereignty impact that?

Leviathan was written shortly after the Treaty of Westphalia. Social structures moved away from feudalism in Europe, and worked toward the formation of nation-states. The Thirty Years War resulted in the Treaty of Westphalia, which is generally credited as the beginning of our nation-state structure internationally. So from Hobbs' view, because of the absolute nature and power of the sovereign, they were all coequal and in a state of anarchy internationally where they interacted without any limitation or rules governing their conduct (sort of a "might over law" point of view). That has changed over time – we certainly know that states have ceded over some aspects of their sovereignty through treaties and customary international law to the international system, but it was the starting point for assessing the significance of the concept of sovereignty with respect to inter-state relations.

Some examples of where that absolute sovereignty and anarchy in the international structure have been scaled back in the 20th century are the United Nations Charter and the Kellogg-Briand Pact, which sought to outlaw aggressive warfare. There are human rights laws and human rights treaties that can penetrate the veil of sovereignty in a state. States agreed that they would limit and put rules on how the state as an entity, and representatives of the state, would treat individuals of another state

with which they were at war (*jus in bello*). And one of the controversial pieces of the Law of Armed Conflict when the Geneva conventions were drafted and adopted, was Common Article 3 which regulates internal armed conflict.

Because of the notion of absolute sovereignty, states conceded, but continued to claim a right to reign supreme within the state's borders. The Geneva conventions, however, came at the end of WWII and the Spanish Civil war where tremendous atrocities in an internal conflict occurred. Common Article 3 – also called the mini-convention – is just one provision; but it essentially says we are penetrating state sovereignty to some degree and binding rules about how you will conduct warfare, even if it is internal warfare. It is seen as the beginning of the human rights movement as well, when taken beyond warfare under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights where states are not completely free to do whatever they want internally.

What does all this say in terms of cyberspace and how it operates and functions with regard to geography, principles of sovereignty, and the authority of states operating in this environment? There are challenging aspects – data flow doesn't easily respect geography, yet there are physical aspects to the internet that are more easily identifiable from a geographic perspective.

A definition of sovereignty taken from a 1928 case of the Permanent Court of Arbitration states: "…sovereignty and relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein to the exclusion of any other state the functions of a state." Interconnectedness raises challenges. Data and privacy issues are getting strained and challenged. When a company subject to U.S. laws houses data in centers all over the world, is that data subject to U.S. jurisdiction? Is that separate and distinct? Can these companies be forced to bring data back? What do other states have to say about this if the data is resident within their borders?

Within the multiple layers and components of cyberspace, nefarious activity (exploitation, disruption and destruction) is increasing. Questions arise about the legal nature of specific acts in the cyber world.

What is the Sony Hack, for example? The presenter said it did not, in his opinion, rise to the level of a use of force or armed attack under the *jus ad bellum*. What is the role of the government in an event such as this? What's the role of the civilian and private sector? Was this just an interference with Sony? It involved destruction of data. It involved ID theft, and the use of that information was different than that usually obtained via commercial espionage – it was used for extortive purposes and to embarrass the company.

According to COL Corn, although the Sony hack was not an armed attack, it was game changing because it was the first time that a dictator – a sovereign of another country – was able to reach inside the boundaries of another state to try and interfere with, through coercive means, the exercise of civil liberties. Sony had the right to publish its movie. Kim Jong Un sought to interfere with the exercise of that right. As such, it may have constituted a violation of the customary international law principle against coercive interventions.

A question emerged from the audience as to whether Japan would have the right to retaliate since the target was a Sony subsidiary located in the United States. COL Corn's response was that it depended on the characterization of what happened, and whether or not the victim has or had a lawful personality of another state. He gave, as an example, the attacks on the U.S. embassies in Kenya and Tanzania. The fact that the targeted embassies were in other countries didn't deprive the United States of the obligation to protect them. The attacks were still considered to be on the United States. This is a more difficult question to answer, however, when the target is or belongs to a private corporation.

But did the Sony hack rise to the level of an armed attack under international law – a violation of article 2(4)of the UN charter which would trigger a right of national self-defense? That's a more challenging question.

What about the use of a U.S. computer to authorize an attack on a civilian in another nation-state? Some hold the view that there is a duty of due diligence on the part of states – leaders can't knowingly allow their territory to be used to commit wrongs against another state – so there is an obligation to stop that sort of cyber activity within a state's territory if there is knowledge of it. Some would argue that there is a

level of obligation to do due diligence in identifying the activity and dealing with it prior to an attack. Proponents of this position argue that it is essentially no different to terrorists operating from within a state's territory, launching attacks against another state. If there is knowledge of such activities and the state from which attacks are launched is unwilling, or unable to do anything about it, then the targeted state has the right to defend itself.

Participants raised the issue of human rights with regard to unauthorized use of equipment to facilitate an attack – is it a violation of human rights for an American citizen to have his or her computer coopted against his or her will? According to COL Corn, arguably so. From a U.S. perspective, if we know there is a botnet deployed on systems within the United States, what are U.S. rights vis-à-vis the botnet and vis-à-vis the state employing it if you are assuming it's a state actor that implanted the botnet? We would have to analyze the inserted malware that allows these machines to be coopted and used in order to characterize the event (e.g. is that an attack on the United States?).

Does Sony have the right to respond? If shots are coming across the border, could you as a citizen fire mortars across the border? Can you authorize companies to start taking action in response to an attack? Who controls the decision about who can bring us, as a nation, closer to conflict? Do we want to outsource that to individuals or private companies? At the level of ambiguity that still exists within cyberspace, that's a very challenging question.

Coming back to sovereignty, there is the question of "unregulated international relations." A1928 case of the Permanent Court of International Justice – the Lotus case – is often cited as a bedrock principle of international law based on sovereignty and the coequal status of states on the international plane. The case involved a maritime accident at sea, Turkish individuals were killed, and Turkey sought to exercise criminal jurisdiction over the captain of the ship (the SS Lotus - a French ship). Effectively the court said that unless something is prohibited in international law, states are free to engage in the activity. That is, international law is essentially a "permissive regime." Turkey exercises jurisdiction within its borders. That is a manifestation of the legal status of the state based on the concept of sovereignty. It can

criminalize and proscribe, and do these things within its sovereign territory. What it can do in relation to other states is a matter of what it, as a sovereign, agrees to in relation to other states.

So in regard to bilateral or multilateral treaties between sovereign equals, a state can surrender some of its sovereignty, it can limit the left and right of what it will do. States can also consent to limitations on their sovereignty through customary international law. It is not written positive treaty law, but when a sufficient number of states adopt and follow a particular course or rule based on a sense of legal obligation, we deem that to be binding on all states.

Therefore, when sovereignty is asserted as a strict trespass rule, it is confusing sovereignty as a concept with a binding norm – a binding legal rule. You have to find evidence of where states have in fact exercised that sovereign right and agreed to limit themselves to find a rule.

One area which is pretty clear is the *jus ad bellum* – the body of international law that governs the right of states between and amongst themselves to use force against each other (to go to war). It's reflected in the U.N. Charter, primarily in article 2(4), which is the prohibition of the use of force or the threat of use of force against the territorial sovereignty and political integrity of another country, carried over from and reflecting customary international law. It is understood, however, that there is a threshold there. It's not *any* affront or perceived transgression. The UN tried to put together a list of what constitutes aggression internationally, but it's certainly understood in the extremes of an armed invasion.

The mining of the harbor in Managua for example was deemed to be a violation of Article 2(4). On the other hand, funding the Contras was found not to be and certain border incursions were not seen to be of sufficient scale and effects to rise to the level of a use of force.

Another complicating factor is that Article 51 of the UN Charter speaks to the right of self-defense. It says that in the face of an armed attack a state can exercise self-defense even absent a Security Council authorization subject to the rule of proportionality. Some states view Articles 2(4) and 51 as two separate standards – armed attack being a higher threshold. The United States does not. The United States views the use of force and armed attack as synonymous, as reflected

in the definitions of hostile act and hostile intent within our rules of engagement (ROE).

Laying aside that there is still some lack of clarity in the conventional sense, and even more lack of clarity in the area of cyber as to what constitutes a "use of force" or an armed attack, there is an understood framework where they are more-or-less aligned. Certain acts, such as economic sanctions for example, don't rise to the level of a use of force or armed attack – you can't respond to an action that doesn't rise to the level of an armed attack with measures that themselves would constitute a use of force or armed attack.

Take Sony for example – if the United States determined that the Sony hack did not have sufficient kinetic effects – that is, destruction and killing in a physical sense – the response cannot include higher measures that would constitute an armed attack. This is essentially the closest (in policy statements) to an equation of what would, in cyber, constitute an armed attack outside of cyber. One should bear in mind that the minute the Rubicon is crossed – in other words, a specific cyberattack is determined to be an armed attack on the United States – the law does not require response via the same medium. If we determine that something happening in cyber constitutes an armed attack, we can –subject to the rule of proportionality – respond with other means to include traditional, military kinetic means.

One also has to distinguish between proportionality in the *jus ad bellum* context, and proportionality in the context of *jus in bello.* The former governs the scope and intensity of a response at the macro level. The latter has to do with weighing the advantage gained by conducting an offensive attack against a lawful target (e.g. military or support to) with the collateral consequence against non-targets.

In addition to the *jus ad bellum,* customary international law also prohibits states from intervening in the internal affairs of another state, specifically against the sovereign prerogatives of that state, through coercive or dictatorial means. The principle of non-intervention – which regulates actions that do not otherwise rise to the level of a use of force – is similarly grounded in notions of sovereignty, but is an actual binding, customary international law norm that states have consented to.

An example: If a state, through cyber or whatever other means, interferes with the ability of another state's voting system (e.g. interfering with elections by rigging voting boxes or systems or taking them down), it would be considered a violation of the principal of non-intervention.

Where do these things fall within international law? Anything that would hit the threshold of intervention or higher would be a breach of an international obligation. That would be a violation of international law unless taken based on a lawful justification. Self-defense, for example is justification when under armed attack. Armed/war measures can be used for self-defense. Countermeasures could be appropriately employed to respond to unlawful interference. Countermeasures can include measures that would otherwise be unlawful, but do not rise to the level of a use of force. Many questions remain about cyber countermeasures – especially with regard to how they might be employed to deal with intrusions and malicious actions.

There is legislation pending that seeks to define what an armed attack in cyberspace is, but to what end? At the end of the day, the National Command Authority assesses the situation and the facts. The President will ultimately decide whether the event is painful enough to respond, and will direct the limits of the response within the existing legal framework.

In order to determine an appropriate response, cyber events must be assessed and categorized. An event/response assessment must consider analysis of a series of questions concerning what is *ad bellum* law and the Law of Armed Conflict (LOAC):

- Acting on a center of gravity analysis may potentially escalate instead of de-escalate a scenario.
- Once you take an action, if what you are doing crosses that line into warfare, the law of armed conflict must be followed (e.g. must be a military objective).

A participant noted that most people do not have issues with internal defense. Everyone can defend themselves. Corporations have a right to secure the networks and they should. The challenge is when individuals and/or corporations decide that the best means of self-defense is to execute offensive operations in order to neutralize the threat.

Messaging an opponent is acceptable. For instance, there is nothing unlawful about the forward deployment of U.S. aircraft, but it is certainly messaging an adversary. When we put a carrier strike group off the coast of a nation-state in international waters – that is messaging from a deterrence perspective.

This type of deterrence messaging is more complicated in the cyber domain. Operationally, in cyber, you have to be on the objective, in over watch, weapon trained and ready to pull the trigger – otherwise you're not going to be effective at the timing and tempo you need to be in a crisis situation. In that context, an initial first-strike could achieve its intention – complete devastation with no capability of response. Therefore, deterrence is crucial. What is the cyberspace equivalent of deterrence?

A discussion ensued about covert action. What responsibility does the state have for individual or group covert actions? Depending on the degrees of affiliation such entities may have to a state's governing bodies, the state may be deemed responsible for the actions of these entities. For instance, from the recipient's perspective, if a bomb goes off and a bridge is blown in another country, the aggrieved state does not care what the U.S. domestic framework says about who executed the attack, or who does what for the government. If the targeted state can prove that the U.S. Government had knowledge of or authored the action, it can respond against the United States.

In the case of a government being responsible for gaining access to a system in gray or red space, COL Corn rejects the notion of a strict trespass rule of international law. Getting those accesses is a lawful option that helps you in posturing for deterrence and other lawful operations – that's a lawful option for the state. How far operators for the state go, what they implant or embed, what the purpose and effect would be with regard to that implant – these details start to move operations across the spectrum and could be crawling up to the line of a threat of force or use of force. At this point, there must be a justification under international law – otherwise, it is transgression.

Private industry now has a conundrum – they are under continual threat, some (as pointed out by several members of the workshop) believe they are not being protected by the state, and feel a need to take

action on their own. On the other hand, response actions are criminal if conducted by private individuals or organizations without authority.

Based at least on the Chicago Convention, flying through the territorial airspace of another country without authority is considered a violation of international law. However, the transit of data across a country's infrastructure is *not* considered trespass (from a legal perspective); although based on international law, countries can make a sovereign decision to put firewalls in place to protect the "territory" within their boundaries and borders.

Does circumvention alone violate the principle of non-intervention? It depends on whether states are reaching in, manipulating, or causing destruction of systems in a way that is coercive to the sovereign prerogatives of the victim state. Remember - what is the means and methods you are deploying – what are the effects – and how does that fit into the schema of international law?

## The Cybersecurity Act of 2015

The Cybersecurity Act of 2015passed a week before Christmas (2015).[80] Antonio Scurlock volunteered to provide workshop participants with an overview of the act and discuss DHS's role pursuant to the Act's designation of authorities.

Title I of the act, entitled "Cybersecurity Information Sharing," establishes procedures of and a framework for data sharing and liability protections associated with privacy. DHS is given the task of codifying practices, clearing them, and presenting them to the public. Under this title, private sector companies are able to share cyber threat indicators and defensive measures with each other and with DHS, under liability protection. They are also given official permission to monitor and apply defensive measures to their own systems (the meaning of which is still under discussion).

Title I includes a requirement for the removal of personally identifiable information (PII) not directly related to the threat data; but it is up to the sharing entity to ensure that PII data is stripped from any reporting. Liability protection is contingent on full compliance with data sharing provisions of the Act. Furthermore, shared information will remain the property of the originator only if designated as such by the sharing entity.[81]

Title II, entitled "National Cybersecurity Advancement," enhances cyber security tools and intrusion detection/prevention capabilities for federal systems, giving DHS the responsibility for collaboration and oversight. This is a step up from the advisory role that DHS had been given by the National Cybersecurity Act of 2014. It also increases capabilities and authorities of the National Cybersecurity and Communications Integration Center (NCCIC), which is the hub for all information sharing in the federal government, while setting procedures for information sharing with the goal of facilitating the process. If cyber security problems are detected within a federal organization, DHS now has a mandate to issue a binding operational directive for correction, as well as to determine a time period within which fixes must be made.

Title III concentrates on "Federal Cybersecurity Workforce Assessment(s)." It is a requirement to assess the number of persons needed to fill cybersecurity and other cyber-related positions.

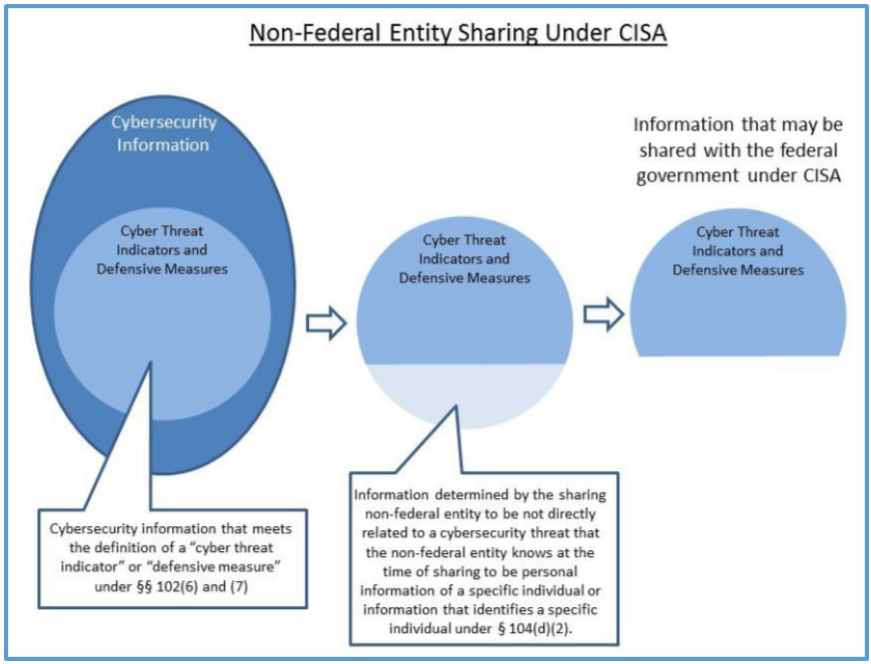
Title IV involves changes to 18 U.S.C. § 1029, providing the ability to bring criminals committing fraud using credit/debit cards (or account information) to justice, providing the accounts are "organized under U.S. or state laws."[82]

CISA provides lengthy definitions, which Mr. Spurlock boiled down to the following:

- Cyber Threat Indicator: An observable (an identified fact) plus a hypothesis about a threat.
- Defensive Measures: Efforts applied to or stored on an information system or information that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. These can be shared and applied to network defenses.

The legal meanings of defensive measures and boundaries are still under consideration. DHS will be holding meetings and tabletop exercises to flesh out the details, while government legal entities determine appropriate interpretations.

DHS is aggressively informing the private sector about the privacy segment of the act. The private sector must make every effort to not share PII unless it is absolutely required to characterize the indicator.




**DHS Office of Cybersecurity and Communications**

Private sector institutions must scrub the information shared to the extent possible. DHS will attempt to clarify what information is and is not desired.

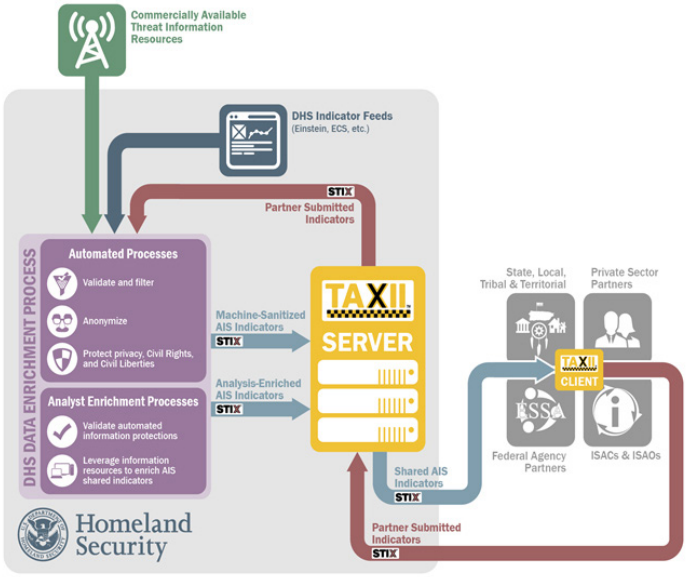
DHS delivered several guidance documents (mostly interim) to Congress on February 16th, 2016. These are also posted online:

- *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government*[83]
- *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities*[84]
- *Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government*[85]
- *Privacy and Civil Liberties Interim Guidelines*[86]

On March 17th, 2016, DHS Secretary Jeh Johnson certified that the automated capability necessary to share information as authorized by the act was operational.[87] The protocol being used by private entities is called Traffic Light, which is a color-based system used to indicate

the level of information sharing required for specific threats. DHS is currently working on a format that will allow for data enhancement/ enrichment during the sharing process.

**The Automated Information Sharing Initiative**




**DHS Office of Cybersecurity and Communications**

The Automated Information Sharing Initiative connects participating (sharing) organizations to a DHS-managed system, which provides information on cyber-threat indicators in near-real time. The intent is to speed up the process of developing defensive measures and adapting systems prior to the enactment of an attack.

The sharing system must also accept web forms that are currently available at the US-CERT website, as well as emails (appropriately formatted or not). Regardless, they all go through the privacy screening. Companies and other non-federal entities that wish to sign up for AIS can do so by contacting taxiiadmins@us-cert.gov for instructions and terms of use. (Participants are vetted.)[88]

**FEMA's National Cyber Incident Response Plan 2.0 (June 2016)**

Mr. Scurlock followed his briefing on the Cybersecurity Act of 2015 with the "reboot" version of FEMA's National Cyber Incident Response Plan (NCIRP) of 2016. The 2010 version of the NCIRP was an interim document.

The new version is intended to address criticisms of the 2010 version which included:

- Reality of response roles was not sufficiently captured
- No plan was included, thus it added little value to response efforts
- There was no interface with the National Preparedness System, specifically the *National Planning Frameworks and Federal Interagency Operational Plans*, for events with both cyber and physical consequences
- There was little clarity as to how external stakeholders, including the private sector and SLTT entities, work together with the Federal Government's efforts
- Industry and government entities have evolved in the cyber arena to include incident response not reflected in the 2010 version
- The federal government has new authorities in government incident response and coordination (*The National Cybersecurity Protection Act of 2014* and the *Cybersecurity Act of 2015*)

The new plan will address the above issues, sync legislation and interagency policy, and address private sector reporting thresholds, procedures, and processes.

NCIRP's guiding principles are:

- Shared Responsibility – Critical Infrastructure/Key Resources (CIKR) are owned by the private sector, so they are critical players in defining shared responsibility for national cyber incident response.
- Risk-Based Response – determining accepted risk for both private and public sector.
- Respecting Affected Entities – by doing blowback assessments (attempting to identify what collateral damage may result from terminating, patching, and mitigating actions).

- Unity of Governmental Effort – attempting to improve inter-governmental cooperation. Still, "whole of government," in reality means a "whole of federal executive government." There is no authority to "touch" the efforts of legislative and judicial branches, with or without their agreement.
- Enabling Restoration and Recovery – by trying to be more preventative and proactive. It is now mandatory for the federal government to have access to certain capabilities.

The "bottom line" goal is to codify a national coordination process for cyber incident response. Although FEMA "owns" the NCIRP, the National Protection and Programs Directorate (NPPD) is teaching FEMA what it means to have a cyber incident and what the nexus between cyber and physical events may potentially look like. FEMA, in return, is teaching the NPPD about the intricacies of communicating during an incident where many layers of government, the private sector, and private individuals are involved, all wanting equal service from the federal sector.

DHS is also in the process of establishing a NCIRP Implementation Working Group, with plans to include representatives from federal cyber centers; Government Coordinating Councils (GCCs); Sector Coordinating Councils (SCCs); SQL Server Analysis Services (SSAs); Information Sharing Analysis Centers (ISACs); and State, Local, Tribal, and Territorial (SLTT) Government Coordinating Councils. Implementation Working Group representatives will be responsible for sharing information on behalf of their respective sector or organization.

**Critical Infrastructure**

A workshop discussion period led to questions with regard to planning and preventing critical infrastructure failure as a worst case scenario. The military looks at the worst case and most likely courses of action (two completely different things) with respect to what an adversary may or may not do. Planners look at both and everything that can be identified in-between; but there may not be sufficient resources to prepare for contingencies. Through risk assessment, the most likely scenarios are identified, and resources are applied in accordance with the assessment. The planning process for any and all potentialities,

is best done in a non-crisis moment, with clear thinking in a calm environment. A good plan provides room for adjustment.

DoD's job is to defeat the enemies of the United States, but also to conduct military operations, from peace to war. In terms of cyber operations across the entire spectrum, thought must be given to capabilities that DoD can bring to the table, the characteristics of threat, and adversarial capabilities.

With regard to cyber warfare, there is an assumption that the military is required not only to consider the day to day threats, but also existential threats. The private sector owns critical infrastructure. If critical infrastructure ends up being the playing field of the next war, and at least part of that warfare is waged with or within the cyber realm (on civil communications, internet, etc.) which is not necessarily under the control of a military command structure, existential vulnerabilities of America rest with the private sector.

As DoD becomes more dependent on civilian CIKR for military operations, is it not safe to assume that a worst-case CIKR attack scenario is considered among the "most likely" scenarios? If the U.S. Government is becoming more critically dependent on the survival of CIKR for military operations and ultimately, to ensure the maintenance of sovereignty, shouldn't it be considered a center of gravity?

One workshop participant cited a private sector tendency which he described as "pre-traumatic stress syndrome"[89] – a reluctance to want to deal with anything really difficult (e.g. hard to contemplate, such as a long-term, catastrophic CIKR outage) – as being in play, especially if private sector would probably not be held accountable for a specific issue, and a business case has not been cited for it. He noted that there is a mental framework which works for the military, but doesn't seem to be applicable (at least not consistently) to the civilian sector, even when both have the same resource constraints. Risk management tends to relieve the public sector from having to consider all scenarios/all options.[90]

The difference is perhaps explained by the military's Clausewitzian view of strategic threat in terms of attacks to the nation's center of gravity, whereas industry (especially utilities) do not think about threat in that manner. The private sector has been forced (by virtue of necessity) to

consider threat in terms of natural disasters, but they don't necessarily see a threat from an enemy as being "their problem." However, adversarial entities can and probably will target the nation's centers of gravity. Thus, what is often referred to as High Impact, Low Probability (HILP) events (catastrophic attacks to critical infrastructure), are actually High Impact, High Probability (HIHP) events in the context of a war scenario.[91]

An attendee noted that a group of economists, engineering physicists, and industry analysts did an economic assessment of low, medium and high impact CIKR events, examining the mean time to replace components across 4 vectors:

1. Large scale power systems
2. Large scale communications
3. Supervisory control and data acquisition (SCADA)
4. Electronics[92]

The study group found that there would be a 40–770 billion dollar loss to the economy in the small area between Richmond, VA and just north of Baltimore, MD before anything was actually repaired, with assumptions that there were no secondary damages (e.g. fires put themselves out and deaths were to be expected normally). This kept the numbers very low to avoid accusations of exaggerated findings.

The most interesting finding was that if the most critical 10% of infrastructure was protected prior to an event, 85% of the estimated economic loss (in this case, the mid-level event) can be avoided. Thus, a risk-based approach to these issues is to assert that it is not that expensive to avoid worst case disasters, such as a catastrophic CIKR event. If you can take the risk-based approach of preparing that 10% in advance, it's not that costly – especially in comparison with doing nothing. The worst case position is a catastrophic CIKR event in which the electric grid will be down long term (potentially, several years). With a relatively small amount of monetary investment and planning, much of the most critical damage could be avoided while building a "resilience dividend."[93]

Finally, a point was made about an earlier comment – there is a military orientation to a worst case scenario that would be instructive for the

private sector, as they have to be given some measure of hope. If you explain the worst case scenario to somebody who's never thought of it before – if you overwhelm them and don't give them hope within the first 30 seconds of the conversation – they "emotionally check out" and default to doing nothing. In private industry, money is the default consideration.

**Developing an Approach**

Joint Publication 5-0, *Joint Operation Planning*,[94] describes operational design methodology and the joint operation planning process (JOPP). Operational design leads the practitioner to "produce an operational approach to guide detailed planning." This approach is informed by an understanding of the environment, as well as the problem. Ultimately, the operational approach is the view of the commander with regard to appropriate usage of government resources to achieve a desired end state.

Participants engaged in discovery about the environment (threat actors) and considered the problem ("factors that must be addressed to change the current system to the desired system"[95]) during the first and second days of the third workshop. Two senior-level subject matter experts were invited to move the process through the last step – to embark on a discussion of the approach for tackling the issues identified by previous guest speakers.

**Singularity**

Jack Tomarchio, co-chair of the Cybersecurity and Data Protection Group at Buchanan Ingersoll & Rooney, PC and former Principal Deputy Under Secretary for Intelligence and Analysis Operations, began the task of developing an approach for future events as a "wrap-up" to the Cyber Sovereignty Workshop series. Having had the opportunity to read Lieutenant General Cardon's article, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains,"[96] Mr. Tomarchio decided to expand on the topic, naming his presentation "The Coming Singularity in Army Maneuver Dominance – Ruminations of a Mere Colonel, Retired."

In the book *The Singularity is Near*,[97] futurist Ray Kurzwell posits that the 21st century will be the most stunning and most exciting epic in

human existence; that we will see the most meaningful thing ever to happen to human beings – a merger between mankind and the machines we build (the singularity).

Kurzwell talks about the fusion of humans and machines as the future of our species. It could be argued that this is happening now, albeit maybe in small ways. Recent advances in biomedical engineering, artificial intelligence, surgical transplants (artificial knees, hips, corneal transplants, etc.) are reminiscent of the 1970s television show *The Bionic Man* – stronger, better, faster.

When LTG Cardon talks about the merger of Army and land maneuver doctrine with cyberspace, he does so in a macro way. Commanders need to think in terms of using cyber operations on the battlefield, they need to become better acquainted with cyber tactics, and consider how the cyber realm is going to be indispensable to the battle commander of the future. Taking LTG Cardon's perspective a step further, the Army needs to think about the realities presented by the emergence of cyberspace on the battlefield as a call for Army senior leaders, as well as DoD senior leadership, to *commit* to the process of melding cyber power and kinetic power into a "battleforce" for the future – like Kurzwell's vision of the fusion of man and machine.

Mr. Tomarchio recalled how the history of warfare is replete with examples of technological advances that change the landscape of battle and how a nation conducts war. He asked participants to consider the following examples:

- The year is 326 BC at the Indian frontier, and the army of Alexander the Great is meeting the army of King Porus at the Hydaspes River. Alexander the Great was seen as invincible and the Macedonian phalanx was considered to be the most advanced military weapon or weapons system of the ancient world at that time. In this battle, for the first time, the Macedonians were challenged with something they had never seen before – the use of war elephants by the Indian army of King Porus. The war elephants didn't break the Macedonian phalanx, but their use broke the will of the Macedonian army and the mercenaries that accompanied them thousands of miles across Asia minor into the beginning of the Indian subcontinent. While the battle was not a loss for Alexander, it was a defeat – Alexander's

soldiers refused to go on. The war elephants eroded their ability to continue the campaign.

- Consider the year 1415 in Agincourt, France, and the use of the English longbow against French heavy cavalry, who rode on war steeds covered with armor. The English archers were able to stand at a great distance. With the great accuracy provided by the long bows (which hadn't been seen before), the archers decimated the Cavalry before they were able to engage with the English.
- Think of the massed artillery fires used by Napoleon during the Napoleonic Wars. Think of the impregnability at Waterloo of the British Squares against the French cuirassiers, and how that tactic ground the Grand Army of Napoleon down to nothing.
- Think of the use of rifle barrels during the 19th century to extend the range and lethality of infantry weapons on the battlefield.
- Think of the German Wolf pack tactics of Admiral Karl Donitz in World War II and how they almost strangled England and changed Naval warfare at that time.
- The book *Actung-Panzer!* written by General Heinz Guderian in 1937 describes the Blitzkrieg tactics that completely overwhelmed Holland, Poland, France, Denmark, and eventually Norway.
- The French had the static Maginot line. They sat waiting for the Germans to throw themselves up against the fortifications as they did in 1916 at Fort Douaumont in the Battle of Verdun. It didn't work, so things changed.
- Think of the use of mass bomber fleets that essentially reduced places like Dresden and Tokyo to ash heaps in 1944/45.
- And finally the introduction of atomic weapons in 1945 that not only ended World War II, but ushered in a new age of potential nuclear Armageddon.

We call these seismic shifts in military tactics, thinking, and weaponry "Revolutions in Military Affairs" (RMAs). Now with the ubiquitous usage of cyberspace, cyberwarfare, and cyber tools, we see another RMA. As Kevin Coleman said, "this is a big thing" and it's changing things really, really fast.

Consider the previous discussions about social networking, and how our whole society is changing as a result, as well as the rise of the stateless state with currency that's no longer tied to a central bank.

*"Cyberspace,"* Mr. Tomarchio contended, "*is not just a bolt-on technology that the warfighter is going to tuck into his rucksack and go off to war with – it's a silent and ever-present actor in the way that we conduct present military operations and think about the future."*

Accordingly, the speaker pointed out three "salient quotes" in General Cardon's article:

1. "We must envision a future where the information environment and the physical environment converge, and adapt our operating concepts to make the most of the opportunities this presents."[98] General Cardon's comments on convergence of the physical, topological, and information environments in future combat operations environments harkens back to Ray Kurzwell's singularity between man and machine. For just as man will become empowered by his singularity with machines, so too will the battlefield commander of the future, gaining greater situational awareness, operational effectiveness, boldness, and the ability to inflict the element of surprise with these new weapons so that he can gain superiority on the battlefield. He will do this in conjunction with and by necessity a *must* with kinetic power.
2. Cardon further notes: "Future dominance on land, by its very nature, will require dominance in cyberspace. To achieve mission success, Joint and Army commanders must possess a basic understanding of the cyber domain and how it achieves inter and intra domain effects."[99] Rather than a basic understanding, however, future army commanders will have to become a master of the world of cyberspace and its use in conjunction with kinetic weaponry.
3. Lastly he notes: "We must understand cyberspace as a warfighting domain, and demonstrate maneuver in this domain both independently and in support of land operations. With this in mind, what does our future force look like and how does it fight with and through cyberspace? To remain the world's dominant

> landpower, the army must reimagine how it conducts 21st century unified land operations."[100]

These comments, are very important but perhaps they don't go all the way. They get to the 50 yard line, but how do we go beyond the 50 yard line? To effectively fuse cyberspace operations into the warfighting lexicon of the Army, we must radically reorganize our thinking about combat operations and how cyberspace plays a key role in future warfare.

In the 1970s, the battlefield of the future was called the Airland Battle Concept. In those days the enemy was the Warsaw Pact. How would the Army close with the Warsaw Pact hordes, made up of Armored, Guards, East German, Polish, and Bulgarian Divisions, rushing through the Fulda Gap? By mastering the Airland Battle Concept the battlefield commander of the future would achieve battlespace dominance and eventually victory. That called for utilizing the coordination between tactical air forces and the troops on the ground – in many cases armored infantry and of course, artillery.

As tactics progressed, the Airland battle concept developed into an Air, Land, and Space concept, where space enabled weapons and space communications were added to the mix. Now a new element – cyber – is injected into the battlespace. To be successful in tomorrow's wars, we must plan, train, field and exercise cyber operations; but how do we do that? Army doctrine will have to be rewritten to make cyber more integral to the battleforce. General Cardon doesn't really talk about that, but he does allude to it. In essence we must rewrite Army doctrine to address the Cyberland battlespace concept.

How do we do that? We need to recalibrate the force itself. Recruiting the right people and retaining them will be extremely important, although difficult. Cyber brings its own unique recruiting challenges. In the past, the Army recruited young men who were good on the football team; but with cyber and other new technologies in the mix, perhaps different choices need to be made. How does the Army recruit the non-athlete or the "mathlete"?

Is anybody satisfied with the personnel issue with regard to cyber? Does anyone think we have the personnel, the training, the jointness?

Further participant discussion on recruiting and retaining a cyber force raised the following points:

- Perhaps what is needed is a change in the tactics, techniques, and procedures (TTPs) because the technologies are already here. How do we integrate cyber operations with all other operations? How does it become a synchronous operation?
- There are six core joint functions that must occur in every domain for you to be a successful joint warfighter: Command and control, Movement and Maneuver, Gather Intelligence, Sustain, Protect, and Coordinate Fires. All of that must therefore be done in cyberspace if it truly is a domain. The tenets of warfare apply in cyber as they do in air, land and sea.
- Training takes 18-24 months – how can the services get a return on their investment when recruits have extremely marketable skills at the end of their tour of enlistment? From another point of view, the competition is more about numbers as all organizations are recruiting from the same pool. With a few exceptions, the salary differentiation is more of a myth than reality, plus the private sector can't offer the sense of fulfillment (e.g. interesting mission).
- Is retention necessary, when youthful energy and ambition may be the most valuable asset for cyber soldiers? Alternatively, will the services achieve their objectives with a rotating cyber force?
- The services have a lot to offer individuals if we catch them at the right time with the right mindset – graduation from college is not the right time to capture their mind.
- The DoD needs people with technical backgrounds and also people with an understanding of national security – few are able to get training to do both.
- Many of the technology students in universities today are foreign-born; therefore, they can't get clearances. How do we solve this problem?
- A couple of years ago, the GAIC (Global Information Assurance Certification) had a cyber warfare certification, but they have since stopped offering that. There are many cybersecurity certifications, but none for cyber warfare or cyber strategy. Cybersecurity is very important for the private sector but for the government you need

> to have a strategy to conduct cyberwarfare and there is no way except by entering the military or one of the relevant agencies to get any prior training or knowledge, with the possible exception of a few Masters degrees that provide courses in cyber strategy.

It always comes down to people – to the force. What does the force look like? Maybe it is a blended force. It will obviously have a large cyber component. It's going to affect critical infrastructure. But the battlefield is going to include civil society – so the battle is going to have to be fought, not by just a bunch of green suiters, blue suiters, or even purple suiters, but a bunch of gray suiters.

How do you deal with that? How do you get people into the force and keep them? Are you going to train them differently, recruit them differently? Maybe they'll do active duty for a couple of years and then go into the reserves for another 12 – thus, the vast bulk of the cyber force might be reservists. This model is used in our Civil Affairs units. Maybe they will get some kind of professional pay. Maybe their basic training will be much different than that which other recruits can expect. Regardless, the services must be able to envision a world where they are not in competition with private industry, but in a hand-in-glove partnership with them, because private industry is going to be in the battlefield.

Perhaps a new branch is in order – a Civil Affairs Branch? Is that a possible topic of a follow on conference? How do you get kids coming out of colleges and universities to look at a dual track between the military and civilian sector? This is a very difficult problem to solve – we don't have the bodies.

**Transformation and Sovereignty**

Brigadier General (retired) Jeffrey G. Smith Jr., former Deputy Commanding General for Proponency, United States Army Cyber Command, currently Deputy Superintendent of Academic Affairs and Dean of the Faculty at Virginia Military Institute was invited to share his thoughts on transformation with regard to cyberspace operations. His presentation on this topic to a previous USAWC workshop was a tremendous hit, sparking great enthusiasm for an update.

BG Smith's style of delivery is so unique that it is difficult to catch the intriguing nuances of his ideas in summary. Thus, an edited transcription follows:

> *By the time you've had a number of years in [the military], you end up talking about how to transform that institution. So I think whenever you get into anything related to proponency, doctrine, or to organizational constructs, concepts, theory, that are rooted in a particular institution, you get to know the life cycle and the battle rhythm associated with how much time it takes.*
>
> *What's the source of resources, or what are the processes, who do you go to in order to get permissions, or what kind of tiger teams do you have to build? You make mistakes in a variety of ways and by the time you are a senior leader, you know what you want to do, how long it will take, and what kind of change you can essentially visit upon your home institution.*
>
> *But when you enter the world of academics, the question is really how do you change a faculty? At VMI we have 140 full-time tenure track professors and that translates to about four or five that change out every year. So you hire them in a particular discipline for their particular background and the content of each of their courses reflects a particular classical view of the world. (The minute you've graduated from college you have a classical view of the world that's got to be constantly updated.)*
>
> *How do you change an academic institution? It's got a very different battle rhythm, source of resources, different timing, and yet if you don't change the educational construct, you're going to have a very difficult time with the subject matter that we're dealing with today.*
>
> *It's not a training issue – it's an educational issue; and of course, an experience issue. I don't mean to denigrate training, but I don't think you can train one in the kind of attitudes that we are talking about. You've got to change the college as well.*
>
> *A topic I've become most interested in is the security of human beings – the collective security and long-term prosperity of human beings.*
>
> *I'm interested in the field of the survival of beings like ourselves. I don't even call us human beings anymore because there are futurists that get*

*into the discussion of singularity where man-made technologies allow you to transcend your physical limitations to the point where you, in fact, evolve your own species. I don't want to preclude that discussion from taking place, so I'll say human beings for now – but that's the broader subject. And how do you secure this particular species? The way we do it today is by securing them by groups.*

*We happen to be associated with a nation called the United States. But the minute you get overseas or are a part of NATO, you begin to take on a huge empathy for other nations and the next thing you know you have a global flavor. There are other groups that are not interested in being a nation, but you have empathy for their needs and requirements and so on. It's a series of human groups that are struggling for survival and that's the broader context for this discussion of cyberspace.*

*So that's what I'm going to talk about today and I think it's got everything to do with why I went to VMI because I'm interested in the educational layer that takes place at the crucial ages of 18-24 or 25.*

*The background I come from is land cyber – we built a concept in the early stages that talks about convergence of the physical world; we're Army so we called it Land (LandCyber), but you should see, in parentheses, the words Air, Sea and Space. The physical world, tied to the cyber world which increasingly I see as our virtual activity – our virtual behavior – is no less real than our physical being. It is characterized by human intelligence. It's really the core of what we would call in the Army, Battle Command. You've got to build your particular networks around leaders, their missions, and their technologies (these networks are your cybercrafts), and then you've got to connect them – every relevant group as well as the machines that are relevant to your survival. Then you need to organize. The vast majority of engagement and interaction that takes place is through information, so you've got to organize it.*

*If you were to take a still photograph of our gathering today, there would be very little physical activity, but all sorts of information is being organized as we speak, into patterns that are useful to each of you individually. We do that in order to escape our physical limitations or to reinforce those capabilities that we already have.*

*We take for granted the shape that we've already imposed on the physical universe. Many people call cyberspace the "only manmade domain" but that is really a misunderstanding – it takes for granted all of the shaping we've done on the physical universe. We've built bridges, we've built roads to facilitate our passage, we've built material, we've built motorized vehicles, airplanes, etc., in order to be able to shape the natural environment to our needs. And then we impose our will on it to some extent. We shape information into force. We sense a general competition in the struggle for survival and we've built powerful capabilities – we call them forces – and then we apply them as leaders in this land. We must understand the physics, chemistry, biology, geology, topography, ecology, culture and social laws that govern life on land and in the virtual realm.*

*Notice I said the virtual realm. I think anything short of that is looking at the world through a classical perspective. We lead on Land (Air, Sea, and Space) and in Cyberspace. It's the equivalent of staring across the Fulda Gap from the Soviet side with a pair of binoculars during the Cold War. What is the Russia/Chinese counterpart to the Cold War doing today? Where are their binoculars? They're in our systems.*

*And we bump them for that – we call that "acts of war." Did we call peering through a binocular in the Fulda Gap an act of war? No – we called it common sense. So this notion that we should be responding in some kind of powerful kinetic, cinematic way for them doing the only thing they can do to keep ahead of something that moves at the speed of light – which is to be at the point of origin – is it appropriate? How else are you to stay ahead of it?*

*I think that warfare in cyberspace is different than warfare in the physical domain. What constitutes an act of war in cyberspace? The fact that we have difficulty with that question is that we don't imagine this other world which says "my virtual presence is important here." I must be there virtually in order to effect and account for a potential physical attack.*

*What do I mean by converging the physical and the virtual worlds? An act or an effect in one has consequences in both – that's what I mean by convergence. If you do something in cyberspace, if it's converged, it*

*will have an impact on some information or object in cyberspace, but it will also have an effect on the ground. That's convergence.*

*The effect of a digital "attack," changes your whole attitude, your psychology, and it could also change your assumptions. If you're getting information that has been altered in some way, suddenly the assumptions of your decision-making have changed.*

*Let me give you an example – a Robot, before it receives its processor is just a simple physical machine. The minute we add a processor, we've converted that machine – we've given it a brain. We instruct the brain and the brain then converts that physical machine into something that acts as our surrogate. The minute you do that you're in a world of convergence. Convergence we take for granted.*

*You receive an email that relays information in a narrative voice that you are familiar with – your loved one – that relays the death of a child. This is an act of convergence. That news would be conveyed in a very different way many years earlier. If you see cyberspace as distinct from the physical world and your physical presence, then you've underestimated what's happened here.*

*You are receiving information objects that take on a very real psychological meaning for you – that change and alter the course of you as a person, and if you're a leader of a large organization, the activities of those organizations. When you consider those alterations with respect to all of the interaction that's going on out there, it becomes impossible to predict. Like the butterfly effect, things change in such a way that it is beyond your control (at least with our current capabilities) to even predict the results. Predictive analysis becomes quite problematic in a fully-realized, converged cyber and physical world because the data set is incomprehensively large.*

*I'm assuming that everything has been "cyberized" – that is, everything has been converted that is capable of being converted (converting its essence into digits or information that can then be analyzed). But yes – convergence is almost so obvious that people struggle with it, when in fact in the most simple sense, we have been living for some time as physical beings who act and behave virtually in cyberspace. In the last few years, we've gone from struggling with our distinct duties of intelligence, signals, cyber, and we're trying to figure out how these*

*constructs fit together; but the idea of convergence is really central to taking cyberspace seriously.*

*What do we mean by the virtual environment? We've been struggling with the physical environment for years and years and we came up with fundamental forces to shape that behavior – army forces, air forces, space forces, naval forces. But we don't even have a name for the virtual environment other than cyberspace and the vast majority of human beings don't talk about cyberspace – they talk about the Internet. Futurists talk about cyberspace as a part of singularity; but in the military, we speak about cyberspace as an operational domain, albeit from a very small perspective.*

*What about a security plan? As part of a good security plan, you need to conceive of an environment that is large enough for your subject. For instance, if your subject is survival, you've got to have an environment that accounts for all the threats to that survival. You've got to get a universal image in your head.*

*Imagine a few hundred years ago when there wasn't a single human being on earth that could fully conceive of being part of a planet spinning thousands of miles per second on an axis, circling the Sun, which itself was circling part of multiple sets of discs that are on the outer edge of a galaxy that itself is part of a cluster of galaxies, and then a supercluster of galaxies all held together by four basic fundamental forces. No one could conceive of that 400 or 500 years ago; and to this day we understand that image but we're much more comfortable with understanding rivers and roads and smaller kinds of elements. No physicist, no one who is a serious scientist can operate successfully without that broader context of the physical universe.*

*We haven't done anything like that with regard to explaining the virtual world. You're going to have to account for the fundamental forces that shape your behavior and then identify the various elementary particles (physical and virtual) that combine into your relevant objects – easy to discuss in the physical world. We all understand, to some extent, quarks, electrons, atoms, and molecules, planets, and humans – but what we still haven't been able to do is account for the behavior of the human being – human psychology. The objects that really dominate the virtual world are human beings and the way we think. We need a*

*field theory that unifies an understanding of the physical universe and an understanding of human nature.*

*With regard to the physical universe – there has long been a search for a Unified Field Theory that accounts for the behavior of all physical forces. They have a model for it – and that model includes the forces of gravity, electromagnetic force, weak and strong nuclear forces, it includes all the particles, and these equations largely (for the most part) explain the behavior of all physical matter in the universe. The gaps are the things that they are still searching for. Seventy to ninety percent of matter remains unaccounted for in the universe – this is called "dark energy" or "dark matter" and they're searching for it. They're trying to figure out if there is a single equation that accounts for quantum behavior and gravity.*

*What they are not seeking are the equations that explain how humans behave – the equation for intelligent life. Consider cyberspace as information objects that are coded, and these codes create objects like worms and viruses and bugs and robots and emails and visual second lives and financial systems and traffic control and visual maps overlaid on air so that airplanes understand what airspace means – the particles of cyberspace are code written by humans endowed with intent designed to shape the way we behave and the way we think and the way our machines perform.*

*So cyberspace, unlike the physical universe, is trying to account for the way humans behave and think. It's intelligent space, and intelligence is the most problematic and dangerous aspect of human security that we have. What we need is some kind of a unification – an understanding of these two.*

*I believe that mathematics is the language of the physical universe. So I think that they are very much partners in crime in all this, right? Information sciences are essential to this – computer and information sciences are teammates in this. There is no "lead" as such.*

*We do have, though, an image that in the Army is called the operational environment. I think it's poorly used – I think you ought to use it more. It's everything that is relevant to a commander's decision process, and what the commander's decision process is based on is a mission. The ultimate mission is to secure the long-term prosperity of*

*that human group. Elevate that to the operational environment as the environment in which humans compete for survival – just a slight, but distinct difference. You've scaled it to the universal, and whatever domains you choose to divide it into should account for all threats and opportunities.*

*Here is the way we've broken it down in the DoD: "A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander" (JP 3-0). Although it's not elevated it to the universal level, they've narrowed it down to commanders. They've divided this area into 5 domains (Air, Land, Sea, Space, and Cyberspace) which essentially gives the impression that everyone's got about a 20% "skin in the game." There is no visual I think that has ever really accounted for these. And when the DoD starts getting into a description of this new thing called cyberspace, it reads a lot like a network (e.g. "an operational domain composed of computers, processors, programs, networks, spectrum, the things they operate, and their human operators").*

*The operational environment can be rescaled to say:*

- *Humans live and behave physically on land, in air, sea, and space, and behave virtually in cyberspace*
- *They lead converged lives*
- *Cyberspace is the virtual counterpart to the physical universe, and like it, is expanding*
- *Eventually, all things and living beings are connected physically and virtually*

*In the same way that you understand we are on a spinning globe on an axis circling the sun and so forth, you theoretically see yourself as part of these constellations. That image is not necessarily in our heads at all times. I think the same thing can be said about convergence – we should take it for granted, but in order to take it for granted in a constructive way we need to remind ourselves of what convergence means.*

*What is cyberspace? I think cyberspace is the virtual counterpart to the physical universe. It's expanding with it. And eventually you'll have to assume that anything that is a physical object, can in fact be*

*connected, and subsumed and converted into this world and vice-versa.*

*Cyberspace is scaled to everyone and everything. It can be scaled to group discussions, it can be scaled for the purposes of the Army, but its infinitely scalable as a consequence of the fact that its particle matter is intelligent data.*

*There is convergence of a physical being into a vast variety of aliases that live distinct from you, and in certain respects they act different and have different consequences in cyberspace. You now have to account for their actions in both cyberspace and as a physical being. Identity in cyberspace is fundamentally fractured in so many different distinct areas and pieces of data that to think that you can preserve the singularity of your physical identity in cyberspace is absurd. They will recombine you in a variety of ways for their purposes.*

*The key law is: "an effect in one world has consequences in both." I couldn't emphasize this more. I believe there are laws associated with cyberspace that we will eventually begin to have to document the same way that we document the laws of the physical universe, which again is the focus of the physical scientists. That's why they are interested in mathematical equations. But there are laws that have the same bearing and weight and majesty in cyberspace as they do in the physical universe. Some will be mathematical in nature.*

*It's not codified – and when I say codified if you continue to see the world as the physical world without these distinctions as to what constitutes virtual behavior and the consequences of that virtual behavior, how is it governed differently? And what is warfare in that kind of environment? What is the financial industry? Why is that different in cyberspace than it is in the physical world? I think what we're really talking about is taking the basic knowledge centers and extending them to examine the extent to which the laws will be modified in cyberspace. There is an element of modification that takes place.*

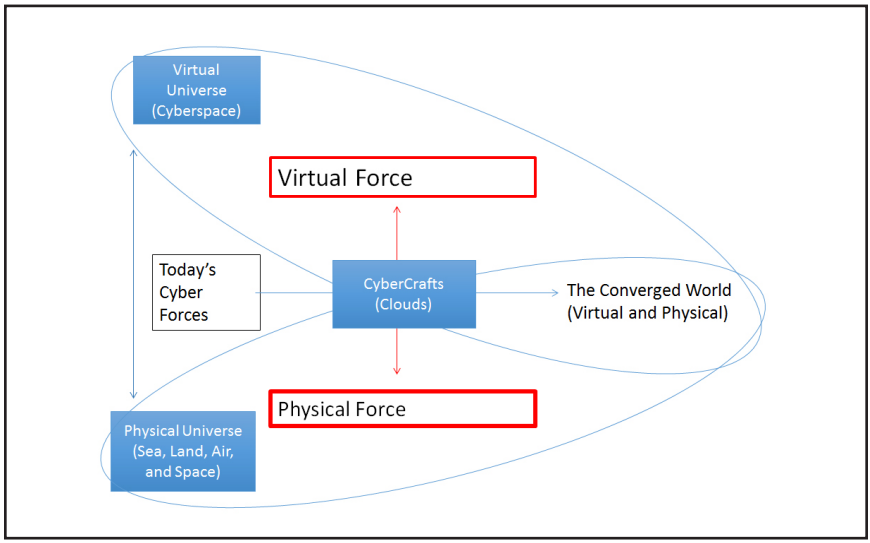
*The fundamental observation is profound – that we are dealing with human nature in cyberspace. It's a different manifestation of it – it's a human nature that has figured out how to build information objects that act on its behalf. But there are consequences, because of*

*the interaction engagement that may change some of the expectations or laws associated with individual disciplines that in their totality express human nature. I'm not willing to close the book yet on the laws that may emerge, but I believe that they are fundamental in nature and I think they'd be recognizable to many of the people that lead the academic department in most schools and universities.*

*The observation made in this room that political science is dealing with it is accurate. The problem is that it's not accurate for every college and every university. We developed our first course in cyberspace as it applies to political science and international studies at VMI but it's not going to be introduced until next year. And the examination of the impact of virtual behavior and virtual organizations is just beginning.*

*I argue that human nature is really the subject matter of its intelligent space. I believe that you have to examine it from that perspective – it helps you to begin to understand actions in cyberspace. I think human nature is endless – it's been endlessly translated into a series of disciplines and knowledge bases. I'm not interested in categorizing them at this point. But you would be amazed at how many of the audiences with whom I speak are still surprised by the notion that cyberspace is made up of intelligent space – made up of information objects that have been designed by humans, endowed with intent and motivation. Cyber is probably distinct from some categories in that it is operational in nature – it's designed to shape and influence, and it has operational information weaponized. I believe it's a category of information that is slightly higher than the basic atomic building blocks of the physical universe*

*There are different kinds of laws, right? There is a law of human nature that says just because its mathematically logical doesn't mean that a human's going to follow it. I think if we discount the notion of science as being absolutely essential in our understanding of human behavior, we really make a large mistake. A simple law like the one that I put up here that said what has an effect in one world has consequences in both is a different category of law – and I'm not even sure if law is the right word. It's this notion that the body of human knowledge has got to start being applied to the way humans have*




*evolved into essentially a virtual world that is continuous – constantly reshaped, but continuous.*

*I think that the social sciences are linked to the physical sciences and at the fundamental level they are governed by the same sort of laws. There is a danger of mistaking complexity and obscurity for some sort of fundamental difference. Physical realities are difficult to understand because we've always been creating this sort of intelligent space that you're now seeing have expression in cyberspace. We exist, to an extent, in our own heads, that's what norms are about, that's what all this is trying to describe, so you can't point to it and compare it with something that's as hard to find as an electron. But those complex relationships are there. It's not something that is ignorable because it is a law of reality in the same way that the laws of physics are.*

*What's the fundamental difference between the internet and letters, books, and newspapers? I look at every one of those things as part of the virtual word. The difference is that cyberspace has a way of converting them rapidly through mathematics into something that can be shared. You can then create weapons and tools automatically that suddenly shape and train, or rip out terrain and replace it with something else, achieve a different end, put you at risk or suddenly give you an opportunity you didn't expect and do that based on aggregations and interactions that are incomprehensible in the analog world.*

*This is a visual that says we have the physical and the virtual – they have their own identities, their own worlds, and you're going to have to create force. You're going to have to be able to navigate in both worlds, These cybercrafts, these clouds, they can be scaled so the level of a tank commander is able to see beyond his turf, or they can be scaled all the way to a large cybercraft (Battlestar Galactica is the one I used 4 or 5 years ago) that can hover and convert the physical world into virtual views that essentially enable them to see as far back as the big bang. It's up to you.*

*You can create all sorts of objects with programs – you can create effects and change the landscape. I think that the competition that exists today is right in the center. This is where you disable and enable.*

*Right now it's sort of like the feudal age before the Westphalian nation-state emerged. You have Google and Apple and you have people that have their own cybercrafts, their cloud equivalents like Microsoft, their own thinkers like IBM's Watson – and in exchange for money they will give you certain services only given to citizens of nations. They'll defend your information. They are in competition with our government right now for those services because they can do things that the government can't. Cyber Command is precluded from defending the citizens of this state. There are issues of sovereignty and there are what I'll call the issues of classical law, that are in the way of behaving securely in cyberspace. Classical law has not yet modified itself to the point where it has begun to fully understand the multiple jurisdictions that include rapid law enforcement.*

*I think we have to temper how we are judging the virtual world by what the corporate world says they do and what they say they are able to do. In other words, I would argue the fact that even the definition of cyberspace, which implies pilotage or control, is that once you abdicate your cognitive and you enter into the cyber realm, you cede control. Are we arrogant enough to think that individuals will be able to exercise a degree of control in the virtual environment when others are trying to do the same thing, let alone achieve dominance – and if not, why would we call it a domain if you can't tactically dominate?*

*The fact that we are pursuing something to tactically, let alone universally, have dominance in an area is a kind of consensual*

*hallucination. Maybe it's a necessary framework for us to progress; but in the end, I agree that it's as much hallucination as ancient people thinking they are bringing the sun back by sacrificing a virgin.*

*Can you control the physical universe? I don't feel any control over the physical universe, although I guess we could through cyberspace or through chemical elements, build some sort of thermostat that might affect it; but we probably have no idea of the potential consequences. Regardless, I don't think you can control the virtual world. I think the minute you create universal images, it's beyond control. The issue is how you shape it, how you operate, how you secure yourself in these environments that are beyond control.*

*This is a fundamental question and may be one of the emerging laws of cyberspace. You're really just trying to do the best you can, which is why we've organized ourselves in these imperfect Westphalian states and why, to some extent, we're adjusting. It's why people escape to cyberspace – to establish their own kind of hegemony and/or organizational constructs. Cyberspace is as large as you are able to imagine, can be scaled in numerous ways which all coexist, and can be changed instantaneously. If you're looking for an escape, that's the place to go.*

*There are countless examples of people who are assembling a piece of terrain in cyberspace on your behalf – that's what they like to do. They'll create that kind of passage through cyberspace and/or they'll create it permanently in cyberspace because that's your real interest. Information objects against other information objects as opposed to let's say influencing the way a view or a user might consider it.*

*There are a lot of competitors in this particular world and I have no idea the shape it's going to ultimately take. We won't know until we get the political scientists, the economists, and business organizations to examine these kinds of worlds. Until you begin to examine it from each of the classical sciences, I don't know how you absorb it.*

*Something powerful has happened and yet the work done on simple geography, cartography, political science, etc., is minimal. I'm doing my best to participate in helping a dialogue that says in the same way that we spent four, five, six hundred years trying to figure out where*

*the earth ended, or where an ocean began, we're just beginning to discover the related associations in cyberspace.*

*So we get back to this basic question – what is cyberspace? I don't think anyone understands it and your response depends upon your perspective. I think if we had this discussion for 5 or 6 or 7 hours all of your perspectives on cyberspace would end up becoming valid. Why? Because you are users – and not only that, you are members of it. You are citizens in your own way and you've got portions of your identity being used whether you know it or not.*

*I went to the Fairfax retirement home and gave a similar brief on cyberspace to people who averaged 91 years old. The vast majority of them didn't use any electronic devices; but by the end of the brief, they became fully aware that they were completely implicated in this virtual world. Their lives were streaming in full vitality as if they were 25 years old, in cyberspace tied to critical infrastructures that existed only in files on servers protected by other information objects that acted like warriors.*

*To the current definitions of cyberspace that are out there I just added about five:*

- *Obviously, the realm of electronic communications – that to me is more in close proximity to the DoD description / definition of cyberspace. A metaphor for the Internet, so to speak.*
- *An operational domain is an example of what that realm could be converted to for the purposes of a smaller subset.*
- *A metaphor for describing the non-physical terrain created by computer systems. In other words, these computer systems give way to virtual reality – suddenly you're in communication with just about anyone you wish.*
- *The consensual hallucination shared by billions of humans – the notion that you're in a collective consciousness which lends itself to singularity and a variety of other kinds of constructs.*
- *And then, virtual reality – the notion of "Second Life" is the way many people think about virtual reality, but really, if you take a look at the Second Life from ten or fifteen years ago, that whole concept is already there – the entire critical infrastructure has been*

*converted in cyberspace from which most of critical infrastructure is controlled.*

*So there are multiple definitions – there is this implication that things can be occupied, controlled and secured – that this operational environment is essentially something that a commander dictates. But those who are not associated with the military speak about an Internet, and futurists talk about singularity.*

*This is intelligent space. I'm providing an example of convergence in terms of cyberwarfare, but this is intelligent movement. You have to create an object and you have to shape the terrain in much the way that space time is shaped. So you create based on gravity, the movement of light, the movement of planets, forced into that movement based on their relationships in terms of gravity; you create tunnels and limit movement; you remove terrain, you give terrain. And that's all done with the creation of information objects that can transform into the equivalent of valleys and peaks, rivers, oceans and bridges and opportunities.*

*Some people figure if they are off line they aren't in cyberspace and I think that's foolish. I think you have to determine that (again, getting back to some laws of cyberspace), potentially all things tend toward cyber, or all things tend toward discovery, and you have to treat potential energy the same as actual energy. Converting something that's not connected to cyberspace for its particular physical uses – it's going to happen.*

*I've just talked about cyberspace – now we're into the problem of cyber. We talk about cybersecurity – it's typically an adjective and a noun for some and a verb for others right? We're still trying to settle our minds on that. We do understand cyberspace, but we've kept our options on the table, so to speak.*

*Almost everything to do with cyber, they say, has to do with computers; but it really has to do with the operational nature of information. When you talk about cyber, someone is up to something. It's not creating inert information or a bunch of data that has to be analyzed – that data hasn't yet been endowed with the intent to shape or influence. I did my best during my early days of conceptual work on this to turn*

*cyber into all information. That did not work. So I've been throwing this out for a few years and it's generally beginning to stick*

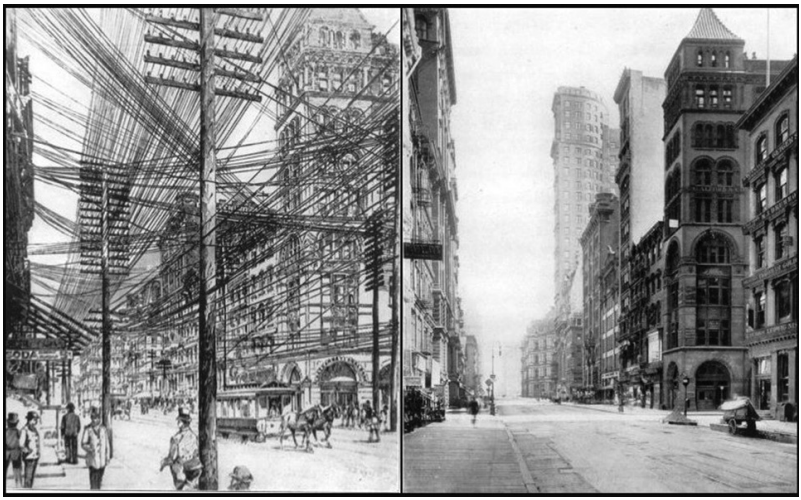
*Human surrogates could be activated – I'm going to build a geographical space that forces and conforms you to go to a particular piece/turf of the cyber infrastructure that's to my advantage. But a surrogate is an object nonetheless – I've created it. I could create an object in the form of an email which is very straight forward. Hardly any subterfuge involved. I now edit and recognize that I'm not there at present so I choose my words carefully and in the act of choosing, I remove something of myself. It's a model of what I would do if I were in person because I would emote if I were talking to you directly; but nonetheless, it's an information object. Therefore, you should treat it with some scrutiny, recognizing it's a surrogate, and not only that it's a surrogate, but that it may have been created as a surrogate by some other surrogate.*

*3D printing has helped us a lot – you convert a physical object into 0s and 1s, or you take 0s and 1s and create whatever it is you want to produce. As noted earlier, a robot, given some code, becomes a surrogate. And then there is the concept of shaping geography, which can look a lot like physical space, or like the time/space element.*

*The creations are so powerful that we've made some adjustments recently. These adjustments are so critical that we're at the point where we feel threatened. We feel we're in danger – that the enemy has infiltrated at the point of entry. The danger is in part, in all of our motherboards, inside of our code. Hoover Dam could be taken over with the loss of many thousands of lives. Water supplies can be poisoned from a distance. But why hasn't all that happened?*

*I think we've failed to adequately account for human nature in this discussion. Once we understand the nature of cyberspace – that it's intelligent space occupied by human beings using objects that have the same intent and motivation as elsewhere – I think that understanding why certain things happen and others don't becomes a little more clear.*

*At the top of the next page is one of my favorite pictures – this is what happened. I can't remember the name of the city, but one day this artist's rendition was created and about a year and a half later, the wires had been moved underground. The infrastructure was visible –*



*it was all part of physical space – and suddenly it was consumed by the background. Now, in our wireless/WiFi world we have to remind ourselves that the notion of an airgap is non-existent today. Even 6 or 7 years ago, if you were in the military and you had an airgap you were fine. But really, it's the electromagnetic spectrum to which you can apply code and withdraw code with a sensitive antenna. You are surrounded – essentially, completely permeated by – at least part of the physical terrain associated with cyberspace.*

*I look at everything as virtual territory. Every one of the objects we have in this room is a source of processing, source of code, and quite frankly could be used for good or for ill. This is the consensual hallucination.*

*There is a dark side – currently known as the Darknet. Ninety percent of cyberspace as we know it is not part of a normal Internet search – but they are building a directory for the Darknet. On the Darknet, there is anonymous travel. You can cover your steps and meet just about every kind of human being. It's a place where people escape. Sort of like the dark energy of the physical universe, the behavior that goes on there is outside of our scrutiny.*

*The laws that govern how we use the Internet are going to shape the scale and scope of cyberspace. These "East Coast laws" are going to shape the geography and your behavior in cyberspace:*

- *If Cyberspace is a metaphor for the Internet, then the laws include the governing bodies of the Internet and computer-related sciences.*

- *If Cyberspace is a virtual counterpart to human society, then the classical laws of sovereignty and jurisdiction, and the social sciences are essential.*
- *If Cyberspace is a metaphor for collective intelligence, then the law of human nature shapes all activity.*

*If it's a counterpart to human society it gets us into the social sciences and the humanities. You are going to have to understand why humans have created the surrogates they have and why those surrogates are interacting the way they are in virtual space. And I think its slightly different – we all know from a psychology perspective that anonymity lends itself to different behavior than when you're engaged in the same behavior in public, in the physical realm.*

*When you convert a thought or a plan into an information object, and include certain people, behavior changes. The study of psychology needs to expand to consider all of that. There are pockets of study along these lines, but not what I would call a formal part of a vison in many schools. If you are struggling with how to deter or shape behavior or influence in cyberspace, get back to the basic notion of intent behind everything.*

*In conclusion, this is about as fundamental a change as you are ever going to come across. The virtual world has been with us since human thought but in leveraging nature's own infrastructure which is the electromagnetic spectrum – the most pervasive energy in the universe, short of dark energy – everything has changed, in my opinion. We're dealing with this forever.*

*As I look at it, cyberspace is an act of collective survival – the opportunity to take brains, and say "humans-you figure it out." We've removed the physical constraints associated with it. The old way of doing business is to organize based on geographical borders (which you just grow up with and either accept or revolt for 700 years). You can now escape to a place where you can help initiate change). There is an element of me that says this is an act of collective survival, but there is another element which says, this is a place where human nature is on full display, for better or for worse, and there is no predicting the outcome.*

*But I believe that this is a decades/centuries-long search – an age of discovery to begin to apply the classical sciences and begin to have them*

*explain a universe which is really tied to the most difficult subject of all, which is human intelligence.*

**Findings and Recommendations**

Workshop participants were asked to recommend areas of focus for future research, workshops, exercises, roundtables, etc. What are the critical areas where the United States should focus cyberspace efforts to achieve its goals? The following issues/topics were recommended and discussed:

- Cyber Sovereignty enforcement.
- Protecting Critical Infrastructure (specifically the electrical grid).
- "Whole of State" response or preemptive integrated operational action taken to mitigate vulnerabilities/weaknesses to the most critical of all prioritized infrastructure assets.
- Pursue development of cyberspace theory which incorporates cognitive sciences and philosophy, and is independent of current operational requirements. In layman's terms: while we're busy trying to keep the alligators at bay, let's have someone focus on trying to drain the swamp.
- How do we fight the next war when we know that cyberspace will be a major component of that conflict; and are we properly preparing our government, our society, and our military to win that next war?
- Can the government (.com, .gov, .mil) identify security standards (SRGs) that should be adhered to? The financial incentives may work – e.g. someone gets a "break" if they are more secure and in compliance with security standards.
- Continue with the development of cyber international law and norms, codified international standards of conduct, and published U.S. responses to violations of standards. These are the ground rules; this is what we will not accept; and this is what we will do if you violate those rules.
- How do we leverage and/or influence cyber education to help address U.S. national cyber challenges?

- We should be thinking about a more comprehensive, integrated approach for government and industry collaboration that addresses needs, resources, and timeframes for those (internally and externally).
- Develop concepts and career paths for cyber systems support teams to assist industry and government operations staffs who don't have time to do persistent cyber analytics, cyber health, and cyber quality control.
- Research manpower and force structure issues; e.g. the development of science, technology, engineering and math (STEM) education connected to hiring processes and educational requirements.
- Better educate and inform the public and private sectors about critical infrastructure vulnerabilities, as they are key with respect to defending the homeland.
- Develop a comprehensive and accepted definition of cyberspace and theory of cyber power including all aspects of sovereignty, security, and offensive cyberspace operations.
- Perform a "whole of government" look at cyber to include the financial sector, both government and private.
- Improve access to STEM career paths for HS students.
- Create education programs for those currently in leadership positions of government and military to increase understanding of adversarial cyber capabilities and limitations.
- Consolidate state, federal, local, and private sector cyber initiatives.
- Increase cyber unity of effort by cyber Command and Control (C2).
- People, Process, and Technology – training, processes, and TTPs in place; work with industry to develop cyber defense tools (to build security up-front, in the design of products).
- Cyber intelligence transformation – to include a better means to declassify so we can share threat information on a non-attribution basis.

- A public diplomacy narrative that clarifies the U.S. position on the legal and policy foundations of cyber sovereignty. Address unauthorized access to critical infrastructure.
- Public debate on the proper role of government, security services, and the military based on our values and principles.
- Cost actuarial risk of cyber vulnerabilities. Figure out what the risks are, and then the costs associated with fixing / not fixing the associated vulnerabilities.
- Don't forget the small guys – defenders and responders (private and public sector).
- Influence digital sovereignty norms and laws in the international law community (custom and case law). Even though the United States isn't a party to the ICC or the ICJ, we've been very influential in the past in making international law. How we define international law today is probably the way the ICC and the ICJ will define it. With our high-tech related cases, understand that what we decide in courts today will influence international law in the future.

Participants were then asked to pull the common themes out of the above recommendations. Commentary included the following remarks:

- One of the main things we need to do is prioritization. We need to find the big, scary risks and work on those first. For the public and private sector, we need a risk analysis – what items, what things put the private and/or public sector at most risk?
- The Russians were able to get to space first because President Eisenhower had to consider legal precedent for overflight. While we had or were very close to the capability for launching first, there was no legal precedent, or we would have set the legal precedent (or caused an international disturbance). Since the Russians did that first, we were ok with that – the legal precedent was established. In the same sense, we may want to go down that road in cyber law and see how that progresses.
- Greater collaboration is needed between the public and private sector – putting them in a position to work these things together in a way that benefits both. Too often, things come as a mandate; and If not a mandate, then a solution that involves industry, but if

industry is not involved in development, implementation becomes a major issue.

- Theory – where is it that we can make a unique contribution? Since most of the other issues listed are being worked on by other organizations, theory is where we could make a unique contribution. Right now, however, it's an area that is being pursued by only a very few.
- We need to codify the strategic communication regarding cyberspace. The discussion by the public is already happening in colleges and universities, so those proponents are molding the future cyber workforce. We need to understand what the public debates are, and who is molding the public debate.
- It seems we're in conflict with the whole notion of cyber sovereignty, when what we really want to achieve and maintain is freedom of operation. The tenets of sovereignty oppose that.
- Throughout this series, we've been looking at cyber sovereignty from the viewpoint of what we already know – we've been using our own paradigms. There should be some kind of mechanism to look for a process or concept that we don't already use (for example using the process of triage for counterterrorism purposes). Is there another way or another discipline that we can use?
- With regard to cyber education, there was discussion over whether STEM was the best target audience for a cyber workforce. There was also a warning about creating compartmentalization of education which could result in the general cyber workforce having a very narrowly concentrated perspective, which was said to be typical of STEM education by one of the participants.
- There is a need to try to reach people of all ages in these fields. Unless you're in the military or government, much is focused on students or recent graduates. The need is for people in the public and private sector, at mid-career and leadership levels.
- Defense Support of Civil Authorities is a contentious issue (as noted in discussions). DoD, DHS, state, and local authorities are all in play – it would be good to get all of the right individuals at the various levels in the same room and ask the right questions.

> What are the expectations and what are the obligations in a time of crisis? The nuances need to be worked out. Put together a concept of operations as a workshop outcome – none exists at this point.

What are some great ideas for future workshops and/or conferences? We as a group have come up with some ideas, or a vision of what our next conference could or should be. Our thoughts were based on: critical infrastructure (electrical grid and finance), cyberattack, and Cyber Protection Teams that are starting to be allocated to Guard units. We're in FEMA Region 3 – hopefully we could get some FEMA folks to come, get Homeland Security support, and get the State Adjutant Generals involved. Intense discussion ensued:

- It was noted that State and FEMA regions operate very differently, and the Adjutant Generals often have different authorities, thus it is difficult to generalize findings.
- Additionally, a participant commented that grid components are different, SCADA systems are different, and cooperation between private utilities and the military to the extent that they are sharing cyber responsibilities is dubious. This brought up intense discussion, with reference to it being a problem that Admiral Rogers "was trying to get his head around."
- People come up with good plans – which are recognized as such by leadership, and may end up in a policy or other type of document, so there is an intent. But when you get to the level or point where execution is supposed to occur, questions are raised, unintended consequences noted, and the implementation never occurs. What seems to be missing is a mechanism that helps to align intent and execution.
- Regarding the Defense Support of Civil Authorities piece – culturally, the rule of thumb is not to "panic the public." It's not good for the economy. Therefore, there really is no place for the discussion of big "scary" problems. Also, no matter what happens to you in the universe, we have guaranteed that we will rescue any American from anything by "day 4" – have three days of food and water and all will be well (on the DHS website). DHS is beginning to change that (some websites say seven days). The Assistant Secretary of DHS has co-chaired a task force at the White House

called the National Space Weather Strategy Task Force and for the first time since the demise of the Civil Defense program, we've admitted we may not get there on "day 4." Maybe it's "day 40," maybe "day 400" – now we really have a need for Defense Support of Civil Authorities. One of the goals is to get not only "whole of nation," but "whole of community" involved, because there is wording that reflects the capabilities of many types of attacks to take down the grid (to include cyber). DHS has also come out with a new Regional Resilience Assistance Program focusing on drive-by RF Weapons against the cyber industry. The industry – not government – asked for assistance on that. We still haven't seen "the cyber shoe" really dropping yet with regard to critical infrastructure, when the problem may be so bad that we'll really be in need of Defense Support of Civil Authorities. We're for the very first time, willing to admit the problem publicly, but we're only beginning to work on it.

- We've been talking about many of these things for a very long time. We need to attach ourselves to some entity or organization to get some of these things moving. Although there are incremental changes (e.g. USCYBERCOM's alignment to defend the nation, educational systems, etc.) but a lot of these issues are repetitive. There must be some attachment to taking these to the next step, which is making a difference/making it happen. To some degree the right folks are here, but there needs to be a hook to get the attention of those who really can make a difference. This needs to be pursued with all due diligence. The time is getting short before we really do get to a place where we have no electricity. These are really big issues – we've talked about them in all three workshops – the next step is "make it happen."
- Could we have a "theory to practice" exercise?

That's our challenge – other than having a great meeting with great networking potential, where are we going? What are we going to do? We need to go from debate to delivery.

## Conclusion: Topics for Future Workshops

**IDENTIFY WHERE WE CAN "HAVE AN IMPACT" AND FOCUS THE NEXT EVENT ON A "DELIVERABLE"**

Our goal is to go beyond a forum for dialogue to a group that recommends action based on our findings. We have a process here that allows us to branch out and help our nation. We want to move the ball forward, past the 50 yard line, in whatever avenue that would be most helpful.

The themes noted in the previous section informed the basis for the list of potential follow-on workshops (roundtables, conferences, etc.) as indicated in the list below:

- Critical Infrastructure
- International Law and Norms
- Public/Private Sector – Risk Analysis and Prioritization
- Cyber Theory
- Diplomatic Statement and Communication Strategy to Publicize U.S. Position on Cybersecurity and Incidents
- Cyber Education and Workforce Recruitment and Retention
- Cyber Maneuver Warfare

It was proposed and agreed that we should try to identify one topic. Where can we have an impact? Who is the audience? Who are the people to consult? What would be the deliverable?

# Appendix A: Speakers

## Policy Workshop

**Congressman Scott Perry (PA-4th District)**

Serves on Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee

Pennsylvania Army National Guard, Brigadier General

U.S. Army War College Graduate

**Krista Z. Auchenbach**

Office of the Deputy Assistant Secretary of Defense for Cyber Policy

Formerly Served in the Office of Deputy Assistant Secretary of Defense for Special Operations and Combatting Terrorism

**Ron Plesco, KPMG LLP**

Principal and National Lead, Cyber Investigations, Intelligence, and Analytics Practice

CEO, National Cyber Forensics and Training Alliance

Information Security and Privacy Attorney

Former Federal Prosecutor

**Captain Joel Doolin, USN**

Primary Legal and Ethics Counselor to the Deputy Chief of Naval Operations for Information Dominance

**Peter W. Singer**
Former Defense Policy Task Force Coordinator
Author of:
*Cybersecurity and Cyberwar: What Everyone Needs to Know*

**Major General (R) Robert B. Newman, Jr.**
Senior VP, Sera-Brynn, LLC
Focus on Cyber, Financial and Energy Infrastructure
Former Adjutant General of Virginia
Former VA Deputy Homeland Security Advisor

**Strategy Workshop**

**Major General Joseph A. Brendler**
Director, Plans and Policy (J5) US Cyber Command
Principal Advisor to the Commander, USCYBERCOM
Former Chief of Staff, DISA
Former Director of Operations,
Joint Task Force-Global Network Operations

**Rear Admiral (R) Janice M. Hamby***
Chancellor, iCollege, National Defense University
Former Deputy Chief Information Officer for Command, Control, Communications, and Computers (C4) and Information Infrastructure Capabilities (DCIO for C4IIC)

* Dr. Cathy Downs, Professor of Information Management at NDU's Information Resources Management College, filled in as speaker because Rear Admiral Hamby was unexpectedly unable to attend.

**Major General (R) Jeff W. Mathis III**

Former Commanding General Joint Task Force Civil Support, USNORTHCOM

Former Deputy Director, Anti-Terrorism/Force Protection and Homeland Defense, Joint Staff

Former Commander, Special Operations Detachment, Pacific and JTF-CERFP

**Dr. Mark Troutman**

Director, Center for Infrastructure Protection & Homeland Security, George Mason University

Colonel, United States Army (Retired)

**Joseph H. McClelland**

Director, Office of Energy Infrastructure Security, Federal Energy Regulatory Commission

Former Director, Office of Electric Reliability

## Operations Workshop

**Timothy L. Thomas**

Senior Analyst, Foreign Military Studies Office (FMSO Ft. Leavenworth, Kansas

Former Director of Soviet Studies at the United States Army Russian Institute

Adjunct Professor, U.S. Army's Eurasian Institute and Adjunct Lecturer, USAF Special Operations School

**Kevin G. Coleman**

Emerging Technology Strategist

Former Science and Technology Advisor to the Johns Hopkins Applied Physics Lab

Former Chief Strategist for Netscape

Former Vice President and Chief Strategist of Claremont Technology Group

**Dr. Jan Kallberg**

Cyber Research Fellow and Asst. Professor, Army Cyber institute at West Point

Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas

JD/LL.M. from Stockholm University

**Dr. Milton L. Miller**

Professor, Georgia Institute of Technology School Of Public Policy

Advisory Council, American Registry for Internet Numbers

Member, IANA Stewardship Coordination Group

Former XS4AII Professor for the Security and Privacy of Internet Users, Technology University of Delft, Netherlands

**Colonel Gary Corn**

Staff Judge Advocate, USCYBERCOM

JD with honors from the George Washington University

LLM in Military Law with a concentration in International Law from the U.S. Army Judge Advocate General's Legal Center and School

**Antonio "T" Scurlock**

Director, Cybersecurity Plans & Coordination, Office of the Assistant Secretary, Cybersecurity & Communications (CS & C), Department of Homeland Security (DHS)

Enhance Shared Situational Awareness (ESSA) Lead, DHS

**Jack Thomas Tomarchio**

Principle with the Agoge Group, LLC

Board of Advisors, Drexel Univ.'s Cyber Security Institute

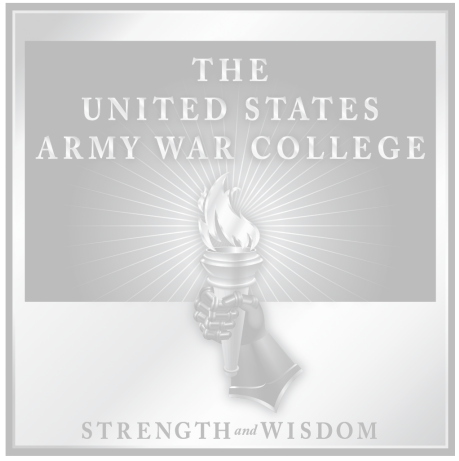
Security Industry Assoc.'s Cyber Security Advisory Board

Former Deputy Under Secretary for Intelligence and Analysis Operations

**Brigadier General (R) Jeffrey G. Smith, Jr.**

Dean of the Faculty and Deputy Superintendent for Academics, Virginia Military Institute.

Former Deputy Commanding General of Army Cyber Command


THE
UNITED STATES
ARMY WAR COLLEGE
STRENGTH and WISDOM

# Endnotes

## Introduction

1. Melissa Hathaway, "Connected Choices: How the Internet is Challenging Sovereign Decisions," American Foreign Policy Interests, Vol 36, pp. 300-313, 2004.

2. Michael S. Rogers, "Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities," http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf (accessed March 5, 2015).

3. Cybersecurity Unit, Computer Crime & Intellectual Property Section, *Best Practices for Victim Response and Reporting of Cyber Incidents*, U.S. Department of Justice, April 2015, http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf, (accessed September 2, 2015).

4. Symantec; *Internet Security Threat Report, Vol 20*; Symantec, 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf (accessed August 30, 2015).

5. For example, see Jens David Ohlin, Claire Finkelstein, & Kevin Govern (Eds); *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford, UK: Oxford University Press, 2015).

6. Mattie Fein, "Congress Should Clear the Legal Fog of Cyber-War," *The Daily Caller*, January 6, 2015, http://dailycaller.com/2015/01/06/congress-should-clear-the-legal-fog-of-cyber-war/ (accessed September 4, 2015).

7. Prescott E. Small, *Defense in Depth: An Impractical Strategy for a Cyber World*, SANS Institute, November 14, 2011, http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896 (accessed August 30, 2015).

8. Bill Gertz, "US Intelligence Community report: America's weak response to cyber attacks will encourage more breaches," *Business Insider*,

July 28, 2015, http://www.businessinsider.com/us-response-to-cyber-attacks-will-encourage-more-2015-7 (accessed August 15, 2015).

9. Ronald Bailey, "Federal Cybersecurity: Not Even Good Enough for Government Work," *Reason.com*, June 26, 2015, https://reason.com/archives/2015/06/26/federal-cybersecurity-bad-enough-for-gov (accessed June 30, 2015); Small, *Defense in Depth: An Impractical Strategy for a Cyber World*.

10. Kevin Coleman, "Private Sector Cyber Ops Getting Hotter," *Defensetech.org,* November 8, 2010, http://defensetech.org/2010/11/08/private-sector-cyber-ops-getting-hotter/ (accessed July 5, 2015); Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed July 5, 2015).

11. Gertjan Boulet, "Cyber Operations by Private Actors in the Ukraine-Russia Conflict: From Cyber War to Cyber Security," *American Society of International Law*, January 7, 2015, http://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber (accessed September 3, 2015); John Grady, "North Korea Looks to Provoke with Cyber Warfare Capability," *USNI News*, September 14, 2015, http://news.usni.org/2015/09/14/north-korea-looks-to-provoke-with-cyber-warfare-capability (accessed September 15, 2015).

12. Jeffrey Hunker, Bob Hutchinson, & Jonathan Margulies, *Roles and Challenges for Sufficient Cyber-Attack Attribution*, Institute for Information Infrastructure Protection, January, 2008 http://www.thei3p.org/docs/publications/350.pdf (accessed August 28, 2015); Bill Gertz, "US Intelligence Community report: America's weak response to cyber attacks will encourage more breaches."

13. Symantec, *Internet Security Threat Report.*

14. Dara Kerr, "Cyber 9/11 May Be on Horizon, Homeland Security Chief Warns," CNET.com, January 24, 2013 http://www.cnet.com/news/cyber-911-may-be-on-horizon-homeland-security-chief-warns/ (accessed May 2, 2015).

15. Warwick Ashford, "Executives Fear Domino Effect of Cyber Attacks, Study Shows," ComputerWeekly.com, 11 May 2015 http://www.computerweekly.com/news/4500246003/Executives-fear-domino-effect-of-cyber-attacks-study-shows (accessed May 20, 2015).

16. James Ryan, "CIA Director Leon Panetta Warns of Possible Cyber Pearl Harbor," *ABC News*, February 11, 2011, http://abcnews.

go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (accessed September 15, 2015); Winn Schwartau, *Pearl Harbor Dot Com*, Interpact Press, 2002.

17. BBC, "US Prepares First-Strike Cyber-Forces," *BBC.com*, October 12, 2012, http://www.bbc.com/news/technology-19922421 (accessed September 10, 2015).

18. Admiral Mike Mullen, "Address by Admiral Mike Mullen" *Carnegie Endowment for International Peace*, September 20, 2011; http://carnegieendowment.org/files/92011_transcript_Mullen.pdf (accessed February 23, 2015).

19. Alexandra Kulikova, "China-Russia Cyber-Security Pact: Should the US be Concerned?" Russia Direct, May 21, 2015, http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned (accessed September 1, 2015); Wu Jiao and Zhao Shengnan, "Xi: Respect Cyber-space Sovereignty," *China Daily Latin America*, July 17, 2014; http://usa.chinadaily.com.cn/world/2014-07/17/content_17814829.htm (accessed March 8, 2015); Alex Grigsby, *Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?* Council on Foreign Relations, January 28, 2015; http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/ (accessed March 8, 2015).

20. Peter Elkind, "Inside the Hack of the Century," *Fortune Magazine,* July 1, 2015 http://fortune.com/sony-hack-part-1/ (accessed Aug 15, 2015).

21. Office of Personnel Management, *Information About the Recent Cybersecurity Incidents,* OPM.gov, June 23, 2015 https://www.opm.gov/news/latest-news/announcements/, (accessed June 23, 2015).

22. Jada F. Smith, "Cyberattack Exposes I.R.S. Tax Returns," The New York Times, May 26, 2015 http://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html (accessed June 2, 2015).

## Chapter One

1. James R. Clapper, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, March 12, 2013, http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf (accessed September 4, 2015).

2. James R. Clapper, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee

on Intelligence, January 29, 2014, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf (accessed September 4, 2015).

3. James R. Clapper, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed September 4, 2015).

4. James R. Clapper, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, Senate Armed Services Committee, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (accessed June 27, 2016).

5. Leon E. Panetta, *Defending the Nation from Cyber Attack,* Speech Presented to Business Executives for National Security, Washington D.C.: U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), October 12, 2012; Deborah Charles, "U.S. homeland chief: cyber 9/11 could happen 'imminently'," *Reuters,* January 24, 2013 http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124 (accessed September 2, 2015); Jake Tapper, "Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War'," *ABC News*, May 27, 2012, http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/ (accessed September 2, 2015).

6. The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*, February 12, 2013, http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf (accessed September 4, 2015).

7. The White House, *Executive Order: Improving Critical Infrastructure Cybersecurity*, February 12, 2013 http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed September 4, 2015).

8. David E Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* June 1, 2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all (accessed September 13, 2015).

9. Jessica Herrera-Flanigan, "Cyber Policy Still Stuck in the '90s," NextGov.com, October 22, 2014, http://www.nextgov.com/cybersecurity/

cybersecurity-report/2014/10/cyber-policy-still-stuck-90s/97184/?oref=ng-channelriver (accessed March 8, 2015).

10. Office of the President, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed February 20, 2015).

11. 113th Congress, *H.R. 624: Cyber Intelligence Sharing and Protection Act*, April 22, 2013, https://www.govtrack.us/congress/bills/113/hr624/text (accessed June 1, 2013).

12. 113th Congress, *H.R. 3696: National Cybersecurity and Critical Infrastructure Protection Act*, 2014, https://www.govtrack.us/congress/bills/113/hr3696 (accessed June 1, 2015).

13. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (accessed June 6, 2015).

14. U.S. Department of Defense, *The Department of Defense Strategy for Operating in Cyberspace*, July 14, 2011, see https://en.wikipedia.org/wiki/U.S._Department_of_Defense_Strategy_for_Operating_in_Cyberspace (accessed June 1, 2015).

15. This was perhaps influenced by a depiction of cyberspace in Russell Fenton's "Content Management Serves as a Vital Cyberspace operations Enabler," *Signal Magazine, Vol 36* (2), 2011, http://www.signal.army.mil/armyComArchive/2011/Vol36/No2/2011Vol36No2Sub06.pdf (accessed 5 April 2015).

16. Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly*, Spring 2011, pp 89-90, http://www.au.af.mil/au/ssq/2011/spring/dunlap.pdf (accessed February 2, 2015).

17. Department of Homeland Security, *Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive-21 – Critical Infrastructure Security and Resilience*, DHS, March 2013, http://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (accessed September 16, 2015).

18. Rep. Michael McCaul, *H.R. 3696 National Cybersecurity and Critical Infrastructure Protection Act of 2014*, 113th Congress, https://www.congress.gov/bill/113th-congress/house-bill/3696 (accessed September 16, 2015.

19. Government Security News, "DHS and DoD sign Cyber-Defense Memo," GSN Magazine, January/February Print Edition, http://www.

gsnmagazine.com/article/21625/dhs_and_dod_sign_cyber_defense_memo (accessed February 20, 2015).

20. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," p. 92.

21. The White House, *Executive Order: Improving Critical Infrastructure Cybersecurity*.

22. Office of the President, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*.

23. Office of the President, *Executive Order: Imposing Additional Sanctions with Respect to North Korea*, January 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea (accessed January 8, 2015).

24. Andrea Peterson, "The Sony Pictures Hack, Explained," *The Washington Post*, December 18, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ (accessed January 8, 2015).

25. Office of the President, *Executive Order 13466 – Continuing Certain Restrictions With Respect to North Korea and North Korean Nationals*, June 26, 2008, http://www.treasury.gov/resource-center/sanctions/Documents/nkeo.pdf (accessed April 3, 2015).

26. Office of the White House Press Secretary, *Statement by the Press Secretary on the Executive order Entitled "Imposing Additional Sanctions with Respect to North Korea,"* January 2, 2015, https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s (accessed January 8, 2015).

27. Joel Doolin, *The Sony Case: The United States Pushes Back*; 11 Feb 2015; A Presentation Given to the Cyber Sovereignty: Policy Workshop, Center for Strategic Leadership, U.S. Army War College.

28. Office of the President, Presidential Memorandum—*Establishment of the Cyber Threat Intelligence Integration Center*, February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat (accessed February 25, 2015).

29. Office of the President, Executive Order – *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,*" April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/

executive-order-blocking-property-certain-persons-engaging-significant-m (accessed April 3, 2015).

30. "U.S. Federal Cybersecurity Operations Team National Roles and Responsibilities," *Introduction to DHS Cyber Efforts*, Office of Cybersecurity and Communications, Department of Homeland Security, March 5, 2013.

31. U.S. Department of Defense, The DOD Cyber Strategy, April 23, 2015, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy (accessed September 2, 2015).

32. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-28: Defense Support of Civil Authorities,* 31 July, 2013, pp. 1-4.

33. Ibid, pp. I-4.

34. Small, *Defense in Depth: An Impractical Strategy for a Cyber World*.

35. Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Criminal Laws*, Congressional Research Service, October 15, 2014.

36. Michael N. Schmitt, Ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, Cambridge, UK 2013 http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf (accessed February 2, 2015).

37. Harold Hongju Koh, *International Law in Cyberspace*, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed February 26, 2015).

38. Ibid.

39. Doolin, *The Sony Case: The United States Pushes Back*.

40. Hathaway, "Connected Choices: How the Internet is Challenging Sovereign Decisions."

41. Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?," *The Air Force Law Review*, *Vol* 64, 2009, pp 1-42.

42. Ben Worthen, Is Cyber Attack an Act of War?, *Wall Street Journal*, August 14, 2008, as noted in Franzese, "Sovereignty in Cyberspace: Can It Exist?."

43. For more information, see Emilie Esposito, "Cyber Crime: The Achilles Heel of the Business World," *Knowledge@Wharton*, University of Pennsylvania, December 20, 2013, http://knowledge.wharton.upenn.edu/article/cyber-crime-achilles-heel-business-world (accessed 11 June 2015).

44. Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No 2; Cybersecurity," October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed March 19, 2015).

45. Andrew Ackerman, "U.S. Chamber Warns Cyberattack Disclosures Could Hurt Corporate Profits," *Wall Street Journal*, October 29, 2014, http://www.wsj.com/articles/u-s-chamber-warns-cyberattack-disclosures-could-hurt-corporate-profits-1414609209 (accessed March 20, 2015).

46. For an example, see: Malia Zimmerman, "Records From Government Data Breach Surface on 'Darknet,' Says Expert," Fox News, June 10, 2015, http://www.foxnews.com/politics/2015/06/10/records-from-government-data-breach-surface-on-darknet-says-expert/ (accessed June 11, 2015).

47. Cory Bennett, "Defense Bill Mandates Cyberattack Reporting," *The Hill*, December 3, 2014, http://thehill.com/policy/cybersecurity/225845-defense-bill-requires-cyberattack-reporting (accessed March 21, 2015).

48. Office of Legal Education, Executive Office for United States Attorneys, *Prosecuting Computer Crimes*, n.d., http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (accessed March 21, 2015).

49. Hayley Richardson, "Companies 'Must See Cyber Attacks as Inevitable'," *Newsweek,* February 16, 2015, HTTP://WWW.NEWSWEEK.COM/COMPANIES-MUST-SEE-CYBER-ATTACKS-INEVITABLE-307111 (accessed February 28, 2015).

50. Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP, *Cyber Attacks: Prevention and Proactive Responses*, Practical Law Company, 2011, http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf (accessed February 28, 2015).

51. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," pp 81-89.

52. Ibid, p. 83.

53. For example, see Trefor Moss, "Is Cyber War the New Cold War?" *The Diplomat*, April 19, 2013, http://thediplomat.com/2013/04/is-cyber-war-the-new-cold-war (accessed March 22, 2015).

54. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," p. 84.

55. Ibid, pg. 85-91.

56. PwC (PricewaterhouseCoopers LLP), *Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015*, September 30, 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (accessed March 11, 2015).

57. Cheryl Pellerin, "Alexander: Defending Against Cyberattacks Requires Collaboration," *American Forces Press Service*, October 30, 2013, http://www.defense.gov/news/newsarticle.aspx?id=121030.(accessed (accessed March 11, 2015).

*58. Leon Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City*, October 11, 2012, http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (accessed September 6, 2015); Michael Hayden, "*Michael Hayden on Electric Grid Cyber Security*," C-SPAN, August 6, 2013 http://www.c-span.org/video/?314419-1/electric-grid-cybersecurity-michael-hayden-industry-perspectives (accessed March 6, 2015); Tony Romm, "Janet Napolitano Warns of Cyberattack on Utilities," *Politico*, November 1, 2012; http://www.politico.com/news/stories/1012/83124.html (accessed March 14, 2015).

59. Aaron Ernst, "Is this the Future of Cyberwarfare? Experts Warn That New Malware Called BlackEnergy Could be Used to Sabotage America's Most Critical Infrastructure," *Aljazeera America*, February 5, 2015, http://america.aljazeera.com/watch/shows/america-tonight/articles/2015/2/5/blackenergy-malware-cyberwarfare.html (accessed February 9, 2015).

60. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," p. 85-88.

61. Harold Hongju Koh*, International Law in Cyberspace*, March 25, 2010, http://www.state.gov/s/l/releases/remarks/139119.htm (accessed March 15, 2015).

62. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," p. 85-88.

63. Ibid, p. 84.

64. See Peter Singer's Ghost Fleet: A Novel of the Next World War, (Boston, Houghton Mifflin Harcourt, 2015).

65. Uwe Bott, "Cyber Warfare: The Real Cold War," *The Globalist*, March 11, 2014, http://www.theglobalist.com/cyber-warfare-real-cold-war/ (accessed February 19, 2015).

66. Moss, "Is Cyber War the New Cold War."

67. Ibid.

68. Paul Sarbanes and Michael Oxley, *The Sarbanes-Oxley Act of 2002*, http://www.soxlaw.com/ (accessed February 15, 2015).

69. Department of Commerce, Office of the Chief Information Officer, *Summary of Major Provisions of the Clinger-Cohen Act of 1996*, n.d., http://ocio.os.doc.gov/ITPolicyandPrograms/Capital_Planning/DEV01_003758

70. Department of Homeland Security, *Homeland Security Policy Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD – 7), December 7, 2003, http://www.dhs.gov/homeland-security-presidential-directive-7.

71. Rogers, "*Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities*."

72. Anya Litvak and Deborah M. Todd, "BlackEnergy Malware Threat Has Some Uneasy," *Powersource*, November 11, 2014; http://powersource.post-gazette.com/powersource/companies-powersource/2014/11/11/BlackEnergy-spooks-nation/stories/201411110080 (accessed February 23, 2015).

*73. Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City*.

74. Michael Hayden, "*Michael Hayden on Electric Grid Cyber Security*," C-SPAN, August 6, 2013; http://www.c-span.org/video/?314419-1/electric-grid-cybersecurity-michael-hayden-industry-perspectives (accessed March 6, 2015).

75. Tony Romm, "Janet Napolitano Warns of Cyberattack on Utilities," *Politico*, November 1, 2012; http://www.politico.com/news/stories/1012/83124.html (accessed March 14, 2015).

76. Carol Matlack, "Cyberwar in Ukraine Falls Far Short of Russia's Full Powers," *Bloomberg Business*, March 10, 2014; http://www.bloomberg.com/bw/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers (accessed March 16, 2015); Henry Meyer and Ott Ummelas, "Estonia Asks NATO to Help Foil 'Cyber Attack' Linked to Russia," *Bloomberg.com*, May 17, 2007, http://www.bloomberg.com/apps/news?p

id=newsarchive&sid=abGseMma5MjU (accessed April 23, 2015); Ward Carroll, "Cyber War 2.0 – Russia v. Georgia," *Military.com*, August 13, 2008, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/ (accessed April 23, 2015).

77. Peter Detwiler, "Terrorist Attack Left All of Yemen in Darkness Last Week: Another Wakeup Call," *Forbes,* June 19, 2014, http://www.forbes.com/sites/peterdetwiler/2014/06/19/terrorist-attack-left-all-of-yemen-in-darkness-last-week-another-wake-up-call/2/ (accessed March 18, 2015); Sky News, "Militant Attack Plunges Pakistan into Darkness," *Sky News*, January 26, 2015, http://news.sky.com/story/1414477/militant-attack-plunges-pakistan-into-darkness (accessed March 20, 2015).

78. John Shy, "First Battles in Retrospect," in *America's First Battles: 1776-1965*, (Lawrence, Kansas: University Press of Kansas, 1986), p. 329.

## Chapter Two

1. Aaron Boyd, "SecDef Nominee: Cyber threats require holistic defense strategy," *Federal Times*, February 4, 2015, http://www.federaltimes.com/story/government/cybersecurity/2015/02/04/cyber-part-broad-defense-strategy/22869325 (accessed July 22, 2015).

2. Dighton Fiddner, *Defining a Framework for Decision Making in Cyberspace*, IBM Center for The Business of Government and Indiana University of Pennsylvania, 2015, http://www.businessofgovernment.org/sites/default/files/Defining%20a%20Framework%20for%20Decision%20Making%20in%20Cyberspace.pdf (accessed July 21, 2015).

3. Fiddner, p. 15.

4. Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, The Center on Law and Security, NYU School of Law, October 2014 http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf (accessed September 20, 2015).

5. Ibid, p. 2.

6. Fiddner, p. 17.

*7. The White House, National Security Strategy*, February 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf (accessed June 18, 2015), p. 1; Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City; Michael Hayden, "Michael Hayden on Electric Grid Cyber Security."

8. Boyd, "SecDef Nominee: Cyber threats require holistic defense strategy."

9. Rogers, Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities.

10. Office of the White House, The National Strategy to Secure Cyberspace, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed 3 June 2015).

11. The Department of Defense Cyber Strategy, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed June 5, 2015). The US Coast Guard published a separate strategy during or after the workshop proceedings: The United States Coast Guard Cyber Strategy, June 2015, https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf (accessed August 10, 2015).

12. The White House, National Security Strategy.

13. The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed August 2, 2015).

14. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (accessed June 6, 2015).

15. Cristin Flynn Goodwin and J Paul Nicholas, Developing a National Strategy for Cybersecurity, Foundations for Security, Growth and Innovation, October 2013.

16. The White House, National Security Strategy, February 2015, pp. 1-5.

17. The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.

18. This is reflective of information provided within the introductory memorandum to the 2015 National Security Strategy.

19. The White House, National Security Strategy, February 2015.

20. Ibid.

21. Ibid, p. i.

22. Ibid, p. ii.

23. The White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy, April 2011 https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (accessed August 2, 2015).

24. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, http://www.nist.gov/cyberframework (accessed August 4, 2015).

25. The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011.

26. The White House, National Strategy for Trusted Identities in Cyberspace.

27. The White House, The National Strategy for Information sharing and Safeguarding, December 2012, https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (accessed August 4, 2015).

28. The White House, National Security Strategy, February 2015.

29. Cyber Command News Release, "Cyber Guard Exercise Tests People, Partnerships," DoD News, July 17, 2014, http://www.defense.gov/news/newsarticle.aspx?id=122696 (accessed July 30, 2015).

30. The White House, National Security Strategy, February 2015.

31. U.S. Cyber Command Public Affairs, Cyber Guard 15 Fact Sheet, http://www.defense.gov/home/features/2015/0415_cyber-strategy/cyber_guard_15_fact_sheet_010715_f.pdf (accessed August 2, 2015).

## Chapter Three

1. Lieutenant General Edward C. Cardon, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains," *The Cyber Defense Review,* Vol 1 (1), Spring 2016, pp. 15-20.

2. Deborah Ancona, Tom Kochan, John Van Maanen, and Eleanor Westney, "Three Perspectives on Organizations" (From Module 2, Managing for the Future: Organizational Processes and Behavior, Southwest Publishing, 3rd ed., 2004), www.morassociates.com/itlp/itlp-readings/3_Perspectives.doc (accessed Sept. 5, 2016).

3. Trefor Moss, "Is Cyber War the New Cold War," *The Diplomat*, April 19, 2013, http://thediplomat.com/2013/04/is-cyber-war-the-new-cold-war/ (accessed Sept 5, 2016).

4. The White House, *International Strategy for Cyberspace [Fact Sheet]: Prosperity, Security, and Openness in a Networked World*, n.d. https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf (accessed July 12, 2016).

5. Department of Defense, The Department of Defense Cyber Strategy, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed July 12, 2016) p. 1.

6. Clapper, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, February 9, 2016, p. 3.

7. Ibid.

8. See FMSO website: http://fmso.leavenworth.army.mil/ for several publications, including: Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations;" *Defense Strategic Communications*, Vol 1(1), Winter 2015, pp 11-26; Timothy L. Thomas, *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*, Ft. Leavenworth, KS: Foreign Military Studies Office, 2015; and Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*, Ft. Leavenworth, KS: Foreign Military Studies Office, 2011.

9. Entsiklopediya prava (Encyclopedia of Law), 2015.

*10. Russian Military Encyclopedia*, 1983

11. Nikolai Patrushev, *Interfax*, 25 May 2016.

12. Russian Security Council Secretary Nikolai Patrushev (Interfax, 25 May 2016) as noted by Mr. Thomas.

13. Information Security Outline, *Kommersant*, 10 October 2015.

14. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York, NY: PublicAffairs, 2015).

*15. Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, 2011 (Brochure as described by Timothy Thomas in delivery of his presentation).

16. Ibid.

17. Soldatov and Borogan, *The Red Web*, p. 162.

18. S. P. Rastorguev, *Informatsionnaya voina* [Information War], (Moscow: Radio and Communication, 1998)

19. Thomas, "Russia's 21st Century Information War," p. 11.

20. APT28: A Windo into Russia's Cyber Espionage Operation? *FireEye*, October 27, 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html (accessed August 1, 2016).

21. Stephen Pifer, "Russia's Perhaps-Not-Real Super Torpedo," *Order From Chaos* [Brookings Blog], November 18, 2015, https://www.brookings.edu/blog/order-from-chaos/2015/11/18/russias-perhaps-not-real-super-torpedo/ (accessed August 15 2016); and BBC Europe, "Russia Reveals Giant Nuclear Torpedo in State TV 'Leak'," *BBC*, November 12, 2015, http://www.bbc.com/news/world-europe-34797252 (accessed August 15, 2016).

22. Kim Zetter, "Inside the Cunning, Unprecedented Attack on Ukraine's Power Grid," *Wired Magazine*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (accessed August 15, 2016); and James Temperton, "Hackers Were Behind the Ukraine Power Outage," *Wired Magazine*, February 26, 2016, http://www.wired.co.uk/article/ukrainian-power-station-cyber-attack , (accessed August 15, 2016).

23. Mary-Ann Russon, "Russia Blamed for Crashing Swedish Air Traffic Control to Test Electronic Warfare Capability," *International Business Times*, April 14, 2016, http://www.ibtimes.co.uk/russia-blamed-bringing-down-swedish-air-traffic-control-test-electronic-warfare-capabilities-1554895 (accessed August 15, 2016).

24. Adam Withnall, "'Russian Submarine' Spotted by Swedish Military Off the Coast of Stockholm," *Independent*, October 20, 2014, http://www.independent.co.uk/news/world/europe/swedish-military-sights-russian-submarine-off-coast-of-stockholm-9805097.html (accessed August 15, 2016).

25. David E. Singer and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," *The New York Times*, October 25, 2015, http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0 (accessed August 15, 2016).

26. Mike Gruss, "Russian Satellite Maneuvers, Silence Worry Intelsat," *SpaceNews*, October 9, 2015, http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/, (accessed August 15, 2016); and SpaceNews Editor, "Russian Satellite Maneuvers Illustrate Why U.S. Alarm

Bells are Ringing," *SpaceNews*, November 6, 2015, http://spacenews.com/editorial-russias-orbital-provocations (accessed August 15, 2016).

27. Pierre Bienaime, "Western Space Agencies Are Tracking What Could Be a Russian Satellite Killer," *Business Insider*, November 18, 2014, http://www.businessinsider.com/us-tracking-possible-russian-satellite-killer-2014-11 (accessed August 15, 2016).

28. John Shammas, "Russia Testing 'Suicide Bomber Drone' Designed for Top Secret Kamikaze Missions – And It Will Hit Battlefield Soon," *The Mirror*, May 28, 2016, http://www.mirror.co.uk/news/world-news/russia-testing-suicide-bomber-drone-8075796 (accessed August 15, 2016).

29. Daniel Treisman, "Why Putin Took Crimea: The Gambler in the Kremlin," *Foreign Affairs*, May/June 2016.

30. Jessica Beyer, "China-Russia Cybersecurity Cooperation: Working Toward Cyber Sovereignty," June 21, 2016, https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/ (accessed August 19, 2016).

31. Wang Xiangsui and Qiao Liang, "Fully Calculating the Costs and Profits of War," in *On the Chinese Revolution in Military Affairs*, ed. Shen Weiguang (Beijing: New China Press, 2004).

32. BBC News, "China Internet: Xi Jingping Calls for 'Cyber Sovereignty'," *BBC*, December 16, 2015, http://www.bbc.com/news/world-asia-china-35109453 (accessed August 16, 2016).

33. Huaxia (ed.), "Why Does Cyber Sovereignty Matter?" *Xinhua News Service*, December 16, 2015. http://news.xinhuanet.com/english/2015-12/16/c_134923687.htm (accessed August 18, 2016).

34. Ambassador Liu Xiaoming, "Building a Community of Common Future in Cyberspace Requires Concerted Efforts," speech delivered before the "Cyber 2016" Chatham House Conference, May 24, 2016, http://www.chinese-embassy.org.uk/eng/EmbassyNews/t1366224.htm (accessed August 19, 2016).

35. Ibid.

36. Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Washington, DC: Project 2049 Institute, November 11, 2011).

37. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 2013.

38. Xinhua, "Xi Jinping Gives Speech at Cybersecurity and Informatization Work Conference," China Copyright and Media, April 19, 2016, https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ (accessed September 6, 2016).

39. Beyer, "China-Russia Cybersecurity Cooperation: Working Toward Cyber Sovereignty."

40. Joshua Philipp, "China Security: Under Veil of Cybersecurity, China Looks to Govern the Global Internet," *Epoch Times*, March 29, 2016, http://www.theepochtimes.com/n3/2006286-china-security-under-veil-of-cybersecurity-china-looks-to-govern-the-global-internet/ (accessed August 19, 2016).

41. Tyler Durden, "China Threatens its Economists and Analysts to Only Write Bullish Reports, or Else," *ZeroHedge*, 3 May 2016, http://www.zerohedge.com/news/2016-05-03/china-threatens-its-economists-and-analysts-only-write-bullish-reports-or-else (accessed August 19, 2016); Chris Buckley, "China Military Paper Warns Officers to Toe Party Line," *Reuters*, May 14, 2012 http://www.reuters.com/article/us-china-military-idUSBRE84E04R20120515, (accessed August 19, 2016).

42. Shen Weigung, *Deciphering Information Security*, 2005.

43. Timothy L. Thomas, *Behind the Great Firewall of China: A Look at RMA/IW Theory From 1996–1998*, Foreign Military Studies Office, November 1998, http://www.au.af.mil/au/awc/awcgate/fmso/chinarma.htm (accessed September 25, 2016).

44. Jacob Aron, "China Launches World's First Quantum Communications Satellite," *New Scientist*, August 16, 2016, https://www.newscientist.com/article/2101071-china-launches-worlds-first-quantum-communications-satellite/ (accessed August 19, 2016).

45. Fan Zheng Jiang and Ma Bao An, *The Theory of Military Strategy*, National Defense University Publishing house, 2007.

46. Ye Zheng, *Lectures on the Science of Information Operations*, Military Science Press, 2013.

47. Sputnik News, "China's New Recon Forces: Unprecedented, Highly-Capable, Ambitious," January 19, 2016, https://sputniknews.com/asia/20160119/.../china-strategic-support-forces.html (no longer accessible).

48. Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Ft. Leavenworth, KS: Foreign Military Studies Office, 2012).

49. Timothy L. Thomas, "Geothinking Like the Chinese: A Potential Explanation of China's Geostrategy," September 29, 2011; http://fmso.leavenworth.army.mil/documents/geothinking-like-the-chinese.pdf (accessed October 2, 2016).

50. Timothy L. "Thomas, China's Electronic Strategies," *Military Review*, May – June 2001 http://www.au.af.mil/au/awc/awcgate/milreview/thomas.htm (accessed October 3, 2016).

51. Wang Xiangsui and Qiao Liang, *Unrestricted Warfare* (Los Angeles, CA: Pan American Publishing Company, 2002).

52. General Dai, *New Perspectives on War*, 2008.

53. Andrew Roth, "Russia and China Sign Cooperation Pacts," *The New York Times*, May 8, 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html (accessed September 2, 2016).

54. Ibid (wording taken from Timothy L. Thomas's presentation of June 7, 2016).

55. Alina Selyukh and Camila Domonoske, "Apple, The FBI And iPhone Encryption: A Look At What's At Stake," *NPR*, February 17, 2016, http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake (accessed September 25, 2016).

56. Richard Rosecrance, *The Rise of the Virtual State: Wealth and Power in the Coming Century* (New York, NY: Basic Books, 2000).

57. Worldania, "How to Create a Virtual Country," *Ethereum*, September 2015, https://forum.ethereum.org/discussion/3347/how-to-create-a-virtual-country (accessed August 20, 2016).

58. Jean-Pierre Buntinx, "World's First Virtual Nation Constitution Released on Ethereum's Blockchain," *Bitcoin.com*, February 18, 2016 https://news.bitcoin.com/worlds-first-virtual-nation-constitution-released-ethereums-blockchain/ (accessed August 20, 2016).

59. Bitcoin News, "Is Bitcoin a Currency or a Commodity? U.S. Regulators Confused," *BitConnect*, March 2, 2016 https://bitconnect.co/bitcoin-news/55/is-bitcoin-a-currency-or-a-commodity-us-regulators-confused/ (accessed August 18, 2016).

60. Kevin Coleman, "Virtual States in Cyberspace Increase in Size and Numbers," *Defense System*s, November 15, 2012, https://defensesystems.

com/articles/2012/11/15/digital-conflict-virtual-states.aspx (accessed August 20, 2016).

61. David Gilbert, "School of Hacking: Inside The Dark Web Virtual Classroom Where Anonymous Wants To Become Great Again," *IBTimes*, April 28, 2016, http://www.ibtimes.com/school-hacking-inside-dark-web-virtual-classroom-where-anonymous-wants-become-great-2360403 (accessed August 20, 2016).

62. Anna Dubuis, "Anonymous Declares War on Islamic State after Paris Attacks in Chilling Video: 'We Will Hunt You Down'," *The Daily Mirror*, November 16, 2015, http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030 (accessed August 20, 2016); Kelly-Ann Mills, "Brussels Attacks: Anonymous Declares War on ISIS in Chilling Video Vowing 'We Will Find You'," *The Daily Mirror*, March 23, 2016 http://www.mirror.co.uk/news/world-news/brussels-attacks-anonymous-declares-isis--7615029 (accessed August 20, 2016).

63. Katie Reilly, "Anonymous Declares 'Total War' on Donald Trump," *Time*, March 15, 2016 http://time.com/4258821/anonymous-declares-war-donald-trump/ (accessed August 20, 2016).

64. Coleman, "Virtual States in Cyberspace Increase in Size and Numbers."

65. Rosecrance, *The Rise of the Virtual State: Wealth and Power in the Coming Century.*.

66. Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999).

67. Ibid.

68. See https://www.us-cert.gov/ (accessed August 21, 2016).

69. "Huawei Banned in the United States," *IKnowToday.com*, n.d., http://www.iknowtoday.com/huawei-banned-united-states (accessed August 21, 2016).

70. See https://www.icann.org/ (accessed August 21, 2016).

71. General Keith B. Alexander, *Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities*, March 16, 2011, http://www.dod.mil/dodgc/olc/docs/testAlexander03162011.pdf (accessed August 21, 2016).

72. Department of Defense, J*oint Publication 3-0: Joint Operations*, August 11, 2011 http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed August 21, 2016).

73. Kieren McCarthy, "US Govt Oks Handover of Internet's Control Panel to ICANN," *The Register*, June 9, 2016 http://www.theregister.co.uk/2016/06/09/us_government_green_lights_transition_of_internet_to_private_sector/ (accessed September 5, 2016).

*74. Stanford Encyclopedia of Philosophy*, Carl Schmitt, October 1, 2014 http://plato.stanford.edu/entries/schmitt/ (accessed August 21, 2016).

75. Jan Kallberg, "Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review*, Vol 1 (1), Spring 2016, pp. 113-126.

76. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute, April, 2013).

77. John S. Foster, Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (Washington, D.C.: EMP Commission, April 2008), http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf (accessed August 12, 2013); National Research Council of the National Academies of Sciences, *Severe Space Weather Events – Understanding Societal and Economic Impacts* (Washington, DC: National Academies Press, 2008).

78. John Denison, *Occam's Razor*, n.d., http://www.occams-razor.ca/index.php/about/what-is-occams-razor (accessed August 20, 2016).

79. Dwight Waldo, *The Enterprise of Public Administration: A Summary* (New York, NY: Chandler and Sharp Publications, 1980).

80. 114th Congress (2015-2016), *Cybersecurity Act of 2015*, https://epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf (accessed August 28, 2016).

81. Ibid, 114th Congress, *Cybersecurity Act of 2015*; Law360, "A Guide to the Cybersecurity Act of 2015," Law360.com, January 12, 2016 http://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015 (accessed August 31, 2016).

82. Ibid, Law 360, "A Guide to the Cybersecurity Act of 2015."

83. Office of the Director of National Intelligence, The Department of Homeland Security, The Department of Defense, and The Department

of Justice, *Sharing Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*, February 16, 2016 https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf (accessed September 1, 2016).

84. The Department of Homeland Security and The Department of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cyber Security Information Sharing Act of 2015*, (Revised June 15, 2016) https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf (accessed, September 1, 2016).

85. The Department of Homeland Security and The Department of Justice, *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* (Revised June 15, 2016) https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf (accessed September 1, 2016).

86. The Department of Homeland Security and The Department of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* (Revised June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf (accessed September 1, 2016).

87. Jason Miller, "Sharing Real-Time Cyber Threats Part of Year-Long DHS Effort," *Federal News Radio*, March 17, 2016 http://federalnewsradio.com/cybersecurity/2016/03/sharing-real-time-cyber-threats-part-year-long-dhs-effort/ (accessed September 1, 2016).

88. For more information see www.DHS.gov/AIS, www.us-cert.gov/AIS.

89. For more information the usage of this term in this perspective see Chuck Manto (chuck@chuckmanto.com); Also see: D. Rubin Berntsen, "Pretraumatic Stress Reactions in Soldiers Deployed to Afghanistan," *Clinical Psychological Science*, Vol 3(5), 2015, pp. 663-674; http://dukespace.lib.duke.edu/dspace/handle/10161/12023 (accessed September 6, 2016).

90. Ralph Langner and Perry Pederson, "Bound to Fail: Why Cyber Security Risk Cannot be "Managed" Away," *Brookings*, February, 2013 https://www.brookings.edu/research/bound-to-fail-why-cyber-security-risk-cannot-be-managed-away/ (accessed September 2, 2016).

91. Cynthia E. Ayers, "The Cyber Threat to the Integrated North American Critical Electric Infrastructure," *Testimony Before the Standing Senate Committee on National Security and Defence*, Senate of Canada, April 18, 2016.

92. For more information see Chuck Manto (chuck@chuckmanto.com).

93. Judith Rodin, *The Resilience Dividend: Being Strong in a World Where Things Go Wrong* (New York, NY: PublicAffairs, 2014).

94. Joint Publication 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2011).

95. U.S. Joint Chiefs of Staff, *Planner's Handbook for Operational Design* (Washington, DC: U.S. Joint Chiefs of Staff, 7 October 2011), V-9.

96. Cardon, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains."

97. Ray Kurzwell, *The Singularity is Near* (New York, NY: Viking Press, 2005).

98. Cardon, "The Future of Army Maneuver – Dominance in the Land and Cyber Domains," p. 16.

99. Ibid.

100. Ibid.


FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

http://www.carlisle.army.mil/

CSL Website

USAWC Website