

# THE CYBER DEFENSE REVIEW



The Future of Army Maneuver-Dominance in the Land and Cyber Domains

*Lieutenant General Edward C. Cardon*

The U.S. Navy's Evolving  
Cyber/Cybersecurity Story

*Rear Admiral Nancy Norton*

Embedding Airmanship in  
the Cyberspace Domain

*Major General Burke "Ed" Wilson*



Uncivil and Post-Western Cyber Westphalia: Changing  
Interstate Power Relations of the Cybered Age

*Dr. Chris C. Demchak*

Protecting the Digitized Society: The Challenge  
of Balancing Surveillance and Privacy

*Dr. Janne Hagen*

*Dr. Olav Lysne*

Cyber Situational Awareness

*Maj. Gen. Earl D. Matthews, USAF, Ret*

*Dr. Harold J. Arata III*

*Mr. Brian L. Hale*

Is There a Cybersecurity Dilemma?

*Dr. Martin C. Libicki*

---

INTRODUCTION

A Dynamic Multidisciplinary Dialogue

*Colonel Thomas Cook*

*Dr. Corvin J. Connolly*

BOOK REVIEW

*Dr. Jan Kallberg*

*The Decision to Attack: Military and Intelligence*

*Cyber Decision-Making by Dr. Aaron F. Brantly*

# THE CYBER DEFENSE REVIEW



# THE CYBER DEFENSE REVIEW

---

## A DYNAMIC MULTIDISCIPLINARY DIALOGUE

### EDITOR IN CHIEF

Dr. Corvin Connolly

### MANAGING EDITOR

Dr. Jan Kallberg

### ASSISTANT EDITORS

Dr. Aaron Brantly

Captain Brent Chapman

Colonel Paul Goethals

Major Natalie Vanatta

### CREATIVE DIRECTORS

Gina Daschbach

Michelle Grierson

### ADVISORY BOARD

Colonel Thomas Cook

Chief Warrant Officer 3 Judy Esquibel

Colonel Andrew Hall

Lieutenant General Rhett Hernandez,  
U.S. Army, Retired

Dr. Fernando Maymi

Master Sergeant Jeffrey Morris

Dr. Edward Sobiesk

Colonel J. Carlos Vega

---

### CONTACT

Army Cyber Institute :: 2101 New South Post Road :: Spellman Hall :: West Point, New York 10996

### SUBMISSIONS

*The Cyber Defense Review* welcomes submissions.  
Please contact us at [cyberdefensereview@usma.edu](mailto:cyberdefensereview@usma.edu).

### SUBSCRIBE

Print: [cyberdefensereview@usma.edu](mailto:cyberdefensereview@usma.edu) :: Digital: [cyberdefensereview.org](http://cyberdefensereview.org)

*The views expressed in the journal are those of the authors and not the U.S. Military Academy, the Department of the Army, or any other agency of the U.S. Government.*

*© Copyright protection is not available for official publications of the United States government. However, the authors of specific content published in the Cyber Defense Review retain copyright to their individual works, so long as those authors are not United States government personnel (military or civilian). Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.*

∞ Printed on Acid Free paper.

---

## INTRODUCTION

<b>COLONEL THOMAS COOK</b> <b>DR. CORVIN CONNOLLY</b>	09	Welcome to The Cyber Defense Review—A Dynamic Multidisciplinary Dialogue
--	----	--

---

## SENIOR LEADER PERSPECTIVE

<b>LIEUTENANT GENERAL</b> <b>EDWARD C. CARDON</b>	15	The Future of Army Maneuver- Dominance in the Land and Cyber Domains
<b>REAR ADMIRAL</b> <b>NANCY NORTON</b>	21	The U.S. Navy’s Evolving Cyber/Cybersecurity Story
<b>MAJOR GENERAL BURKE</b> <b>“ED” WILSON</b>	27	Embedding Airmanship in the Cyberspace Domain: The First Few Steps of a Long Walk

---

## PROFESSIONAL COMMENTARY

<b>MAJOR GENERAL EARL D.</b> <b>MATTHEWS, USAF, RET</b> <b>DR. HAROLD J. ARATA III</b> <b>MR. BRIAN L. HALE</b>	35	Cyber Situational Awareness
--	----	-----------------------------

---

## RESEARCH ARTICLES

<b>DR. CHRIS C. DEMCHAK</b>	49	Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age
<b>DR. JANNE HAGEN</b> <b>DR. OLAV LYSNE</b>	75	Protecting the Digitized Society— the Challenge of Balancing Surveillance and Privacy
<b>DR. KAMAL JABBOUR</b> <b>MAJOR JENNY POISSON</b>	91	Cyber Risk Assessment in Distributed Information Systems

<b>DR. JAN KALLBERG</b>	113	Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations
<b>DR. MARTIN C. LIBICKI</b>	129	Is There a Cybersecurity Dilemma?
<b>FRANCESCA SPIDALIERI JENNIFER MCARDLE</b>	141	Transforming the Next Generation of Military Leadership into Cyber Strategic Leaders: The Role of Cybersecurity in US Service Academies

---

## BOOK REVIEW

<b>DR. JAN KALLBERG</b>	167	<i>The Decision to Attack: Military and Intelligence Cyber Decision-Making</i> by Dr. Aaron Brantly
-------------------------	-----	--



# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆





# Welcome to The Cyber Defense Review—A Dynamic Multidisciplinary Dialogue

---

Colonel Thomas Cook

Dr. Corvin J. Connolly

## INTRODUCTION

We are proud to introduce the inaugural print edition of *The Cyber Defense Review (CDR)*. This quarterly journal will generate an intellectual multidisciplinary dialogue through thought provoking scholarly articles and essays on the strategic, operational, and tactical aspects of the cyber domain. The *CDR* will break down barriers and foster innovative solutions to global cybersecurity challenges. This inaugural *CDR* compiles perspectives from preeminent thinkers across the government, industry, and academia regarding potential challenges, impacts, and initiatives for consideration as we come to grips with cybersecurity.

This scholarly effort from the Army Cyber Institute (ACI) at West Point grew out of its commitment to focus on the intellectual properties present in cyber research, cyber education, and cyber outreach. The ACI is a national resource dedicated to engaging the Army, government, academia, and industry in impactful partnerships to solve over the horizon problems for the Army and the Nation.

The *CDR* has already positioned itself as the leading online multidisciplinary cyber journal for military, industry, professional and academic scholars, practitioners and operators. The online *CDR* provides an unclassified venue for content divided into a journal with longer more thoroughly researched articles, and a blog with short engaging thought pieces to stir rapid discussion within the broader community. We publish original, unpublished, relevant and engaging contributed content from across the community.

The print *CDR* journal is a peer-reviewed publication for robust original, unpublished work to facilitate meaningful discussion. Our inaugural issue connects members of our diverse community to cross-pollinate ideas with the intent of solving tomorrow's



Colonel Tom Cook was commissioned Armor and later joined the Army Acquisition Corps. He currently serves as an Assistant Professor and Director of Research for the Army Cyber Institute at West Point. He has led Soldiers in combat and has written on several topics including software engineering, real-time systems, information assurance, and computer science education. He is a CISSP, CEH, GISP, GREM, and GSEC and holds a Masters in Computer Science and Ph.D. in Software Engineering from the Naval Post-graduate School and a Masters in Industrial Engineering from the University of Louisville.

cyber challenges today. It serves as a forum for sound logic, creativity, and innovative solutions to the challenges faced by the global cybersecurity community.

The first of three articles in the *Senior Leader Perspective* section begins with Lieutenant General Edward Cardon, Commander, Army Cyber Command, as he articulates the Army's urgent need to adapt and integrate our operating concepts for the cyber domain. Next, Rear Admiral Nancy Norton, Director of Warfare Integration for Information Warfare, describes the USN's emphasis on cyber security, noting that cyber is an *enduring mission* and the responsibility of every military leader. The *Senior Leader Perspective* concludes with Major General Ed Wilson, Commander, 24th Air Force and AFCYBER, discussion on US cyber reliance, and the Air Force's emphasis on changing to a culture of air-mindedness for cyber warriors. In the *Professional Commentary* section, Hewlett Packard Enterprise leaders Major General Matthews (USAF, Ret), Dr. Arata, and Mr. Hale assert the criticality of cyber situational awareness (SA) to mission success.

Progressing through this inaugural edition, we provide six scholarly articles in the *Research Articles* section. Dr. Demchak from the Naval War College scopes the global cyber landscape. She contends in the era of cyber conflict a conversation must occur regarding the future of the western dominated cyber framework. Next, Dr. Hagen and Dr. Lynes from Norway, provide a thought provoking and timely article on balancing government surveillance and privacy laws. Third, Dr. Jabbour and Major Poisson from the Air Force Research Laboratory, offer a must-read article on risk assessment in distributed information systems. Dr. Kallberg of the ACI brings to *CDR* readers a



Dr. Corvin Connolly is the Editor in Chief of The Cyber Defense Review for the Army Cyber Institute at West Point. Dr. Connolly was the former Director of Government Relations at Air Force Space Command, and an active duty Air Force officer, retiring in 2006. During his Air Force career, Dr. Connolly served in strategic and tactical missile operations, NATO C2, legislative affairs, and created/edited the *High Frontier Journal* for Air Force Space Command. He is a former Senior Manager, Space and Cyber Systems for Lockheed Martin Corporate Strategy & Business Development. Dr. Connolly holds a Ph.D. in History from Texas A&M University.

novel strategy for cyber warfare. Dr. Libicki from RAND Corporation vividly juxtapose global requirements for cybersecurity and cyber warfare capabilities. The sixth and final article in the *Research* section, cyber scholars Ms. Spidalieri and Ms. McArdle, provide *CDR* readers with a comprehensive analysis of US Service Academies and their development of future cyber leaders.

We conclude this quarter's volume with a book review by Dr. Kallberg, ACI research scientist, on Dr. Aaron Brantly's brilliant and timely monograph, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*.

We hope you find this inaugural edition of *The Cyber Defense Review* stimulating and educational, and come to realize both the importance and complexity of the cybersecurity environment. Please explore our future print and online offerings, provide feedback and contribute as we make this the best possible publication in the cyber community. Our next print issue will be published this July continuing the cyber dialogue with articles from General Joseph Votel, Commander of U.S. Central Command, Major General Stephen Fogarty, Commander, U.S. Army Cyber Center of Excellence, Mr. Thomas Harrington, Managing Director and Chief Information Security Officer at Citigroup, and Dr. Catherine Lotrionte, Director of the Institute for Law, Science and Global Security at Georgetown University. As we continue to build upon the intellectual framework created by this journal, we encourage you to join the conversation!🛡️



# THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆



# The Future of Army Maneuver— Dominance in the Land and Cyber Domains

---

Lieutenant General Edward C. Cardon

## INTRODUCTION

*The year is 2025. Just before dawn, several independent 5-man teams from an Army Combined Arms Battalion prepare to launch an attack on a terrorist-insurgent stronghold outside a mega coastal city in a sub-Saharan nation. Before the commander sends in his attack forces, his cyberspace maneuver force has already established a secure communications network using Free Space Optics and Li-Fi and are conducting defensive cyber maneuver to protect and defend key cyber terrain. While monitoring local social media, cyber operators have intercepted insurgent communications, and located their operations center. They begin sending messages on social media to confuse the insurgent network and interfere with their command and control. Next, the cyber operators launch an offensive cyber maneuver, cutting power to the insurgent headquarters. In another offensive maneuver, the cyber force employs electromagnetic pulses to destroy the adversary's electronic systems followed by a Radio Frequency capability to disable all insurgent vehicles. As dawn breaks, the insurgents awaken to the sound and fury of the Battalion's direct and indirect fires...*

**T**his scenario describes a future when the Army conducts combined arms maneuver simultaneously across the land and cyberspace domains. To be ready for this future, the Army must continue to make significant strides so that cyberspace is inextricably linked to the Army's ability to fight and win in the land domain. For decades the Army has eagerly adopted networked technologies to enhance its warfighting capabilities. As a result, the Army's tactical dominance is unprecedented. However, these same technologies are also significantly changing our world, creating asymmetries that profoundly disrupt future operating environments, and the Army's ability to conduct unified land operations. We must look beyond these expected disruptions to understand how they both enhance





Lieutenant General Edward C. Cardon was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. LTG Cardon has commanded at every level from company through division. Prior to assuming command of the United States Army Cyber Command, he was the commander of the 2nd Infantry Division based in South Korea. His education includes a Bachelor's of Science Degree from the United States Military Academy and two Master's Degrees—one from the National War College and the other from the United States Naval Command and Staff College, both in National Security and Strategic Studies. Lieutenant General Cardon is married and has three children.

and become integral elements to how we fight and win. In short, 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.

The Army Operating Concept is a foundational document. 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.

### ***Cyberspace as a Warfighting Domain***

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. Cyberspace is a uniquely man-made domain that includes physical, logical, and cyber-persona layers. Similar to other domains, cyberspace operations allow the Army and the Joint force to maintain freedom of action within the land domain by providing operational commanders additional avenues of approach against adversaries. Conceptualizing cyberspace as something separate or discrete is shortsighted, and isolating cyber within a separate domain is an approach we take at our own peril.

Cyberspace operations are increasingly inseparably linked with operations across all other domains. For example, mission command requires network defense and platform resiliency, air targeting supports, and is supported by cyber fires, and cyber effects allow commanders to set necessary operational conditions for ground based maneuver.

In other words, future war should be imagined across the land, air, and space domains that will occur by, with, and through the cyber domain. Because of these emerging conditions, to dominate the land domain, the Army must also do so in cyberspace.

### ***Maneuver in Cyberspace***

Traditionally, Army maneuver forces conducted combined arms maneuver on land to seize, occupy, and defend terrain in order to achieve physical, temporal, and psychological advantages over the enemy. The Army's Operating Concept now recognizes that combined arms maneuver actually occurs across all five warfighting domains and acknowledges cyberspace operations as one of seven core competencies.

In future operating environments, the full integration of cyberspace operations into our lexicon, organization, and understanding of maneuver is imperative. Commanders will recognize that the principles of maneuver warfare: targeting critical vulnerabilities; audacity; surprise; focus; decentralized decision-making; tempo; and combined arms are equally applicable in cyberspace.

Cyberspace operations also have a critical defensive component. Defensive maneuver in cyberspace includes hardening and re-configuring systems, limiting and protecting network access points, continually maneuvering data, conducting reconnaissance and surveillance on physical and virtual avenues of approach to key cyber terrain, and using passive and active network sensors. Like other domains, the cyber environment is dynamic. We already see in Eastern Europe how Russian cyberspace capabilities can render radio and satellite communications useless, prevent precision fires, and interfere with Global Positioning Systems (GPS). Through denial of service and malware attacks aimed at the opposition, adversaries use online proxies to control their narrative and support their regional objectives. The ability to conduct defensive maneuver will be an operational and tactical imperative in the future as well.

#### **ARMY CORE COMPETENCIES**

- ◆ Shape the security environment
- ◆ Set the theater
- ◆ Project national power
- ◆ Combined arms maneuver in the air, land, maritime, space, and cyberspace domains
- ◆ Wide area security
- ◆ Cyberspace operations in the land domain
- ◆ Special operations
- ◆ The Army operating concept

### ***Cyberspace Operations and Combined Arms Maneuver***

In tomorrow's complex operating environment, combined arms maneuver requires coordinated efforts, both defensive and offensive, simultaneously across all domains.

Commanders must be just as adept deploying cyber effects as they are delivering physical effects. This level of synchronization is not new to our force. The Army has demonstrated unparalleled expertise in the synchronization of fire and maneuver at a decisive point. Our competence at the operational and tactical level is perhaps unmatched. However, our commanders' continued ability to effectively employ all the tools in this cross-domain arsenal in the future faces two general challenges.

First, Army and Joint operations are dependent upon networked capabilities enabled by cyberspace and space-based platforms from the strategic to the tactical level. In the past, threats to mission command have been generally well known and reasonably mitigated. However, the proliferation of technology and decreasing barriers to entry combine to present potential asymmetric advantages a savvy adversary can employ against the Army and Joint force. In the future, our enemies and adversaries will use cyberspace to influence populations, degrade the Army's technological superiority and impede our

---

Full integration of cyberspace operations into our lexicon, organization, and understanding of maneuver is imperative.

ability to communicate, collect intelligence, operate, and execute mission command.

Second, in light of these potential emerging asymmetries, we must be able to not only defend our own critical assets, but turn the technology to our advantage. We will only achieve the level of operational dominance we de-

monstrated in the past if we are able to leverage and integrate cyberspace operations in the future. To do this, the Army must reimagine combined arms maneuver on both the land and in cyberspace. We have to critically examine how we are organized, how we train, and how we fight. Cyberspace operations, information operations, and electronic warfare must become an ingrained component of a commander's scheme of maneuver. Redundant and disconnected communications will take on new meanings.

Therefore, to successfully execute future mission command, the Army must continue operational integration of EW, IO, Cyber, Signal, Psychological Operations and Intelligence to dominate the information environment. In the past, these functions were separated both across staffs and throughout mission execution. The modern battlefield requires these functions to achieve greater operational integration both in planning and execution. This will entail removing organizational and mission command barriers so that these functions become completely integrated. It demands formations designed for rapid task organization through the integration and synchronization of all Army warfighting functions. Ultimately, before synergy of maneuver across cyber and the land domains can be achieved, cyberspace operations will need to be normalized as a regular warfighting capability, and within a commander's vision of the battlespace.

Our adversaries are already adapting and innovating in this way to maximize their own cyberspace capabilities. Today, Russia employs cyberspace capabilities in a world-wide campaign of social media misinformation to shape domestic audiences and achieve strategic objectives in Ukraine and elsewhere. Russian commanders deploy information operations, electronic warfare, social media, and cyberattacks in a decentralized manner that affords them significant operational autonomy. In recent operations, these and other actors have demonstrated the effectiveness of leveraging asymmetric capabilities to overcome their traditional military limitations.

Army Cyber Command continues the important work of integrating cyber capabilities into the Army's conception of maneuver warfare. We are conducting pilot programs at the Combat Training Centers (CTCs) to exercise defensive and offensive cyberspace maneuver. These exercises will inform holistic Army-wide changes to our doctrine, organization, materiel, and training. The next evolution of this initial cyber integration will be significant, generating critical questions to inform how the Army integrates cyberspace capabilities in the "Force 2025 and Beyond." How should the Army task organize to best integrate cyberspace capabilities? Beyond our current Cyber Mission Force construct, will the Army create a Cyber Expeditionary Brigade that can be rapidly task organized to support commanders? Or, will we permanently

task organize these capabilities at echelon? How will the Army institutionalize cyber operations at the CTCs and wargames? Permanent changes in resources and personnel for individual and collective cyber training up through institutional

changes to CTCs will be necessary. Another evolution of this effort started this year, incorporating civilian technology partners into Army experimentation and initiating a Silicon Valley Innovation pilot to explore social media strategies. Finally, how will the Army develop optimal command and control (C2) frameworks to provide cyber capabilities that can enable commanders' ability to dominate on land and in cyberspace? In doing so, how can the Army best realign network command and control to appropriately match existing land domain authorities? These are just a few critical areas Army Cyber Command continues to address as we look toward the "Force of the Future".

---

---

Army commanders must fully  
embrace cyberspace as a new  
maneuver domain to maintain  
our freedom of action.

## CONCLUSION

Determining how the Army will fully integrate cyberspace operations as part of a combined arms maneuver force into Unified Land Operations will be a constantly evolving process. One thing is clear, we have already *crossed the Rubicon* in cyberspace. It is impossible today to effectively conduct combined arms maneuver or Unified Land Operations without leveraging cyberspace. Many of our adversaries are already exploiting the asymmetric advantages they can achieve through cyberspace and quickly adapting their tactics. As part of a combined arms maneuver force, cyberspace operations could significantly amplify the Army's capabilities to prevent, shape, and win. To win on land in the crucible of tomorrow's complex operating environment, Army commanders must fully embrace cyberspace as a new maneuver domain to maintain our own freedom of action and while restricting that of our adversaries. Dominance in cyberspace is essential to win a complex world. ♥

# The U.S. Navy's Evolving Cyber/Cybersecurity Story

---

Rear Admiral Nancy Norton

## A BRIEF HISTORY OF NAVY CYBER

**Y**ou can't pick up a newspaper or view a cable news program without hearing about cyber, whether cyberattacks, cyber defense, offensive cyber, cybersecurity, cyber threat, *cyber Pearl Harbor*, etc. You might think this issue just popped up the last few years. But all the armed services have been thinking about cyber for a number of years, in fact DEPSECDEF John Hamre originally used the term "cyber Pearl Harbor" in the 1990s, SECDEF Leon Panetta repeated it in 2012. The Navy in particular has been thinking about cyber for a long time.

The origins of the military's emphasis on cyber and cybersecurity can be traced back to at least 1996, when Joint Chiefs of Staff Chairman General John M. Shalikashvili, U.S. Army, released Joint Vision (JV) 2010. This seminal publication championed "Full Spectrum Dominance" as the "...key characteristic we seek for our Armed Forces in the 21st century."

JV 2010 stated, "The fusion of all source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations. Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive *picture* which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it."



Rear Admiral Nancy Norton serves as Director of Warfare Integration for Information Warfare. As an information professional, RDML Norton has served in information dominance billets at all levels, afloat and ashore. She commanded Naval Computer and Telecommunications Station Bahrain during Operation Iraqi Freedom. Rear Admiral Norton served as executive assistant to the Chief of Naval Operations from 2010-2012, and most recently as the director, Command, Control, Communications and Cyber Directorate, U.S. Pacific Command. RDML Norton is a native of Oregon and graduated from Portland State University with a Bachelor of Science in General Science. Norton earned a Master of Science in Computer Science from the Naval Post-graduate School and a Master of Arts in National Security and Strategic Studies from the Naval War College, where she was the President's Honor Graduate.

### *Cebrowski and Net-Centric Warfare*

At the same time, the U.S. Navy moved full steam ahead into Information Age Warfare with its own approach, “Net-centric Warfare”, which first appeared in 1995 in the Department of Navy’s publication, “Copernicus: C4ISR for the 21st Century.” The ideas of networking sensors, commanders, and shooters to flatten the hierarchy, reduce the operational pause, enhance precision, and increase speed of command were captured in this document. As a distinct concept, network-centric warfare appeared publicly in a 1998 US Naval Institute Proceedings article by Vice Admiral Arthur K. Cebrowski and John Garstka, and later in the book *Network Centric Warfare: Developing and Leveraging Information Superiority* by Alberts, Garstka and Stein published by the Command and Control Research Program (CCRP).

The introduction stated, “Network Centric Warfare is the best term developed to date to describe the way we will organize and fight in the Information Age. The Chief of Naval Operations, Admiral Jay Johnson, has called it “a fundamental shift from platform-centric warfare.” We define NCW as increasing combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

### *NMCI*

While the Navy was focusing on the warfighting aspects of cyber, Navy leaders also recognized the immense challenges in managing the ever-growing collection of disparate computer networks, which posed a massive security threat. With no enterprise-level oversight, individual commands could buy and install their own computer systems at will.



Local commands were left to manage the security of their systems. The answer to this problem was the Navy Marine Corps Intranet (NMCI), and its follow-on enterprise network services approach, Next Generation Enterprise Network (NGEN). Under the orders of Secretary of the Navy Gordon England, beginning in 1999, NMCI consolidated roughly 6,000 networks, some of which could not e-mail, let alone collaborate with each other, into a single integrated and secure IT environment.

In a 2004 speech, England noted that, “One of the most pressing areas that needed attention was security. It wasn’t just that we weren’t following our own rules; in many cases we weren’t even aware of them.”

### ***Attacks and Threats***

In the years following the standup of NMCI, the topics of cyber and cybersecurity surfaced occasionally, usually coincidental to some specific security incident, and not always connected to activity within Navy or DoD systems.

In 2008, Russia directed ‘Zombie’ infected computers around the world to barrage web sites in the country of Georgia, including the pages of the President, the Parliament, the Foreign Ministry, news agencies and banks, demonstrating that cyberattacks had moved beyond hackers or hactivists to the realm of international geopolitics.

The US military was also targeted that year. Operation Buckshot Yankee responded to an infection from inserting a USB flash drive into a laptop computer at United States Central Command. The flash drive was left in a base parking lot in the Middle East, infected by a foreign intelligence agency with malicious code that spread when the device was plugged in.

In 2013, Mandiant Security Consulting Services released a report documenting evidence of cyber attacks by China’s People’s Liberation Army targeting 141 organizations in the United States and other countries as far back as 2006.

For the U.S. Navy, this series of eye-openers culminated with a major incident in 2013.

Vice Admiral Jan Tighe, Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet (FCC/C10F) talked about the incident in Congressional testimony on March 4, 2015:

*“...we fought through an adversary intrusion into the Navy’s unclassified network. Under a named operation, known as Operation Rolling Tide (ORT), U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber*

---

---

Network Centric Warfare is  
the best term developed to  
date to describe the way we  
will organize and fight in  
the Information Age.



*Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cyber security posture and defensive operational capabilities.”*

For the U.S. Navy the intrusion mitigated through Operation Rolling Tide marked a significant *cyber awakening*.

### ***Task Force Cyber Awakening***

Navy leaders realized our inability to holistically understand, and command and control, its cybersecurity posture across the Navy, beyond just the corporate navy networks, to include combat and industrial control systems. The Navy also lacked a single enterprise authority to manage cybersecurity. These shortcomings manifested themselves in confirmed exploits and lost data, known vulnerabilities, limited cybersecurity situational awareness, and inadequate safeguards.

To gain that necessary perspective, Admiral Jonathan Greenert, Chief of Naval Operations and Sean Stackley, Assistant Secretary of the Navy for Research, Development and Acquisition, chartered Task Force Cyber Awakening (TFCA) in August of 2014.

TFCA was a year-long effort, led by the office of the Deputy Chief of Naval Operations for Information Warfare (N2/N6), under Vice Admiral Ted Branch. The goal was to baseline the cyber security of the Navy across all systems, afloat and ashore, and determine a way ahead to improve defenses. TFCA was tasked to deliver fundamental change to the Navy’s organization, resourcing, acquisition and readiness by extending our cybersecurity apparatus beyond traditional IT to our combat systems, combat support and other information systems while aligning and strengthening authority and accountability.

TFCA formed four Task Groups (TG), each with representation from across the Navy.

- ◆ TG Capabilities reviewed cyber security actions and assessments already underway or recently completed to prioritize investments to ensure that Navy was taking the right steps in the near-term.
- ◆ TG CYBERSAFE constructed a program, modeled after the SUBSAFE program developed by the submarine community following the loss of USS Thresher in 1963. The CYBERSAFE program would apply to a hardened, very limited subset of components and processes and include rigorous technical standards, certification and auditing.
- ◆ TG Navy Cyber Security focused on evaluating current authorities, methods and resources required to best apply rigorous technical standards, certifications and assessments across the Navy.

- ◆ TG Technical used senior engineers from the Navy's systems commands to ensure that robust, common technical standards and authorities were put in place to drive cyber programs and systems.

TFCA prioritized protection efforts based on recommendations from industry, the cybersecurity community and stakeholders, then evaluated hundreds of funding requests for addressing vulnerabilities, with \$300 million set aside in fiscal year 2016, and additional investment in the five year budget, to strengthen the Navy's defenses and improved awareness of its cybersecurity posture.

### ***Navy Cybersecurity Division***

In September 2015, the CNO established the Navy Cybersecurity Division on the headquarters staff (under Vice Adm. Branch's N2/N6 organization) to continue TFCA's transformation efforts. The new division oversees the Navy's approach to cybersecurity, developing strategy, ensuring compliance with cybersecurity policy, and advocating for cybersecurity requirements. The division will also evaluate and prioritize major investments and manage the CYBERSAFE program.

But the Navy cybersecurity effort is not just the responsibility of the Navy Cybersecurity Division. There are a number of other Navy organizations who are critical to the cybersecurity fight and who are making significant contributions to improving the Navy's defenses. They include:

- ◆ Navy Chief Information Officer: Establishes policy and guidance relating to IT.
- ◆ Fleet Cyber Command/U.S. 10th Fleet: Operates, maintains and defends Navy networks and conducts cyber operations.
- ◆ Information Forces Command: Organizes, mans, trains and equips the cybersecurity workforce.
- ◆ Systems Commands: Strengthen cybersecurity throughout the lifecycle of systems with the goal of "baking in" security from the beginning instead of "bolting it on" after systems are fielded.

As Vice Adm. Branch points out every chance he gets, "The cyber threat is real. This fight is ongoing even as we speak; right now Navy cyber warriors are defending against hackers, cyber-terrorist, and nation-state actors. Furthermore, every day the solutions I buy for the Navy as the DCNO for Information Warfare make our warfighting platforms, communications systems, and business systems more connected through cyberspace... and therefore a bigger target."

The Department of Defense alone experiences 41 million scans, probes and attacks per month.

## CONCLUSION

With those last few statements, it is very clear. The Navy's focused effort has come a long way from the days when cyber was looked at as simply an emerging capability that we needed to exploit. Cyber is now a recognized operational domain, alongside the more traditional land, air, surface, subsurface, and space domains.

Within the Navy, cybersecurity is now considered an enduring mission. We have made it clear, in discussions, communications and training, that cybersecurity is now the responsibility of every commander and commanding officer. It is no longer just passed down to the computer professionals behind closed doors in the basement of the building or the lower decks of the ship. Cybersecurity demands an *all hands* effort.

It is very simple, whenever a Navy Sailor, civilian or contractor logs onto a Navy computer or connects to a Navy system, they are in the cyber battlespace.

We must stay in front of the ever-evolving cybersecurity challenges that face the Navy, the Department of Defense, and our great nation.

Now and in the foreseeable future, it is *all hands on deck*. 🛡️

# Embedding Airmanship in the Cyberspace Domain: The first few steps of a long walk.

---

Major General Burke “Ed” Wilson

*Contributing Authors:*

Col Gregory Gagnon, Col Heather Blackwell, Lt Col Michael Medgyessy,  
Maj Andrew Miller, CMSgt Brendan Criswell, MSgt Brandon Oxton,  
TSgt Tavis Ha, TSgt David Sorensen, Ms. Suzette Elliott

Our Air Force’s use of cyberspace has continued to evolve since its beginnings as a defense and academic research project in 1960. Our reliance on this new domain ranges from cyber’s ability to connect individuals and groups globally; to its ability to enable our electrical, transportation and health systems; to its importance in building our Nation’s economic strength; to its ability to spark innovation and technological advances; to its decisive role in supporting and enabling armed conflict. The Air Force’s reliance on this domain is equally matched by our adversary’s intent to exploit our dependence on cyber. The current trajectory of cyber attacks shows increased frequency and increased effect. Cyberspace is an increasingly contested domain and it is imperative that we shift our mindset from a maintenance focus, and instill an operations culture to rapidly adapt to the shifting strategic environment. If the Air Force and our sister Services are to defend our way of life in this contested domain, we can no longer view cyber as a collection of information technology systems. Since the establishment of Twenty-Fourth Air Force in 2009 and its designation as Air Forces Cyber (AFCYBER) in 2010, multiple articles have advocated for cyber-mindedness and the formation of a unique cyberspace culture. Here, headquartered in San Antonio, we have pursued an alternate approach. For the past several years, we have continued down the path of operationalizing Air Force cyberspace organizations by modeling, educating, and mentoring our AFCYBER forces with a culture of *air-mindedness* as we operate in an inherently joint environment.

When we talk about air-mindedness, we refer to “the lens through which Airmen perceive warfare and view the battlespace”.<sup>[1]</sup> That is why as Airmen, it is ingrained in us



Major General Burke E. "Ed" Wilson is the Commander, 24th Air Force and Commander, Air Forces Cyber, Joint Base San Antonio-Lackland, Texas. General Wilson is responsible for the Air Force's component numbered air force providing combatant commanders with trained and ready cyber forces, which plan and conduct cyberspace operations. Twenty-fourth Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network.

General Wilson entered the Air Force in 1985 as a graduate of the U.S. Air Force Academy after earning a Bachelor of Science degree in electrical engineering. He has served in space and cyber operations, planning, strategy, policy, acquisition and combat support. The general has commanded at the squadron, group and wing levels, and served on the staffs of Air Force Space Command and National Reconnaissance Office.

from the first day we put on the uniform that our Air Force provides the Nation and Combatant Commanders the capability to create tactical, operational and strategic effects at distance, and at the speed of need, often through the use of smaller tactical actions. Our AFCYBER Airmen have begun applying this same thinking and mindset to cyberspace whether in friendly or adversary terrain. This has given them the essential tools to assure the five core missions of the Air Force [air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control] in, through and from the cyberspace domain in support of Joint and Air Component Commanders daily.

Today, we are the most capable, respected, and feared Air Force on the planet. But our position and advantage remains tenuously at risk. Adversaries engage our Air Force in cyberspace continuously, probing for opportunities to disrupt or degrade our ability to provide global vigilance, reach and power. To assure our advantage in the air and space domains, AFCYBER has focused on operationalizing how the Air Force maneuvers and commands cyberspace by using proven air-minded processes and procedures. For almost seven decades, our Nation charged the Air Force to deliver superior effects in, through and from the domains of air and space. In the recent past, our Nation extended that charge to operations in, through and from the cyberspace domain. Similar to Airmen operating in the air domain, AFCYBER directs Airmen executing operations 24/7 across a joint operating area that is not only horizontally global, but also vertically multi-domain enabling coordinated effects between air, space and cyberspace.

Air and space operations come with a proud history and a legacy of valor. Our forefathers fought

to gain and sustain advantage in these domains to enable Joint Force Commanders ***freedom from attack, and freedom to attack*** at the operational time and place of their choosing. For decades, we’ve been tremendously successful as an institution in delivering that promise to our Joint Force Commanders. Some argue that is because of our technology, but many of us believe it is because of our organizational culture, a culture educated and inculcated into our Airmen, and reinforced by our methods, operational processes, and unrelenting innovation. This culture drives and sustains our comparative advantage over other Air Forces. This culture is what we have nurtured, expanded into the cyberspace domain, and continue to lock-in with our organizations and leaders. It is the core of what enables us to operate with the speed, agility and precision required in today’s cyber fight, and will enable us to scale our cyberspace operations for tomorrow’s fight.

### ***Operationalizing the force***

Our Air Force cyber forces are low density high demand assets to meet the rising demands of cyberspace, it is imperative that we operationalize all elements of cyber as outlined in Joint Publications: Offensive Cyber Operations (OCO), Defensive Cyber Operation (DCO), and Department of Defense Information Network Operations (DODIN Ops).

As an organizing principle, our cyber forces are either ***cross-functional team of teams*** or

specialized units. Within the Cyber Mission Force, our cross-functional teams, which combine cyberspace operators, planners, developers and intelligence specialists, specifically align to DoD and Combatant Commanders’ mission objectives. Some of these teams are assigned offensive *global strike and ISR roles*, while other teams execute defensive operations. Within the DCO forces, we have honed the ability to rapidly detect and respond to nefarious actors within blue space, while also hardening our defensive perimeter against the adversary.

Within the DODIN Ops forces, we have operationalized our enterprise activities to enable blue force cyber maneuverability and mission assurance via a global force lay down construct that uses a follow-the-sun operating model. The cross functional team of teams construct allows our organization to adapt to the dynamic and contested cyberspace environment. In order to orchestrate these efforts, our ***Operations Center*** (624 OC) issues ***plans and orders*** through a Cyber Tasking Order to assign scarce, and at times highly specialized, resources to the highest priority missions. Executing C2 through a single operations center with plans and orders enables operational prioritization of the efforts of cyber Airmen conducting missions to deliver combat effects in, through and from cyberspace.

---

---

We partner with other DoD agencies to leverage whole-of-government investment in support of joint warfighting.

### *Equipping the Airmen vice Airmen manning the equipment*

In order to sustain the needed pace of innovation, rapid equipment modifications and the integration of new technology at the speed of cyber must become the norm. Shortly after establishing AFCYBER (24 AF), the Air Force delegated unique authorities (with specific budget constraints) to conduct and execute Rapid Technological Operations and Innovation (RTO&I). The RTO&I authorities have enabled us to push ***decision authority (and accountability) to lower levels*** to meet urgent mission needs. It has been key to strengthening our strategy of cross-functional teaming and decentralized execution. Moving forward, our intent is to increase our use of RTO&I and other rapid cyber acquisition processes to meet the speed required to keep pace in this environment—an environment in which Airmen engage the adversary daily.

### *Training the team—Air-minded language and certification*

To facilitate more effective interaction with our Air Components and Combatant Commands, we adapted the AFCYBER lexicon to common Air Force and joint operational language. This shift is not *just to make cyber sound cool*. Instead, this air-minded language enables all Airmen to communicate seamlessly and more effectively with other operators. As the Air Force Chief of Staff, General Mark Welsh, stated during a warfare symposium: “This is the kind of reset we need ... understandable to everybody else in the Air

A critical step towards operationalizing cyber is incorporating more relevant cyber-centric concepts in tech school.

Force ... ***tasking order ... interdiction ... ISR ... defensive fires ... not technical terms ...*** Air Force Terms. This is the reset. It will make it real for all of us.” This strategic shift in how we approach operational integration has led to a significant ramp-up for junior officers and enlisted learning, which in other domains is often taught at the FGO JPME level (joint planning, targeting). In addition to language and lexicon, we teach and inculcate mission

ready crew concepts, and normalized training pipelines consistent with aircrew, missile, and space operations.

Today, we operate a training pipeline with Undergraduate Cyberspace Training delivered by our Air Education and Training Command (AETC), and weapons system Initial Qualification Training, which is at our user command Field Training Unit (FTU). More specialized Mission Qualification Training is conducted either at the FTU or the gaining unit, which complements the training and mission certification of our intelligence specialists inbound to our cyber units.

A critical step towards normalizing cyberspace operations is the continued incorporation of advanced concepts in technical training school, which better equips our



Airmen for the challenges they face in an increasingly contested operating environment. This crew training normalization necessitated a shift from Quality Assurance to an AF Standardization and Evaluation programs for crew qualifications, proficiency and currency. This cultural shift is still in progress, but gains are very noticeable. This year, our lead operational units will have the full complement of Cyberspace Weapons Officers focused on tactics, techniques and procedures across all lines of operations. Ready Cyber Crew implementation is revamping our recurring training, force presentation and crew risk management strategies.

This more ready and able cyber-space operations force has rightfully generated more demanding collective training requests. In addition to our strong commitment to joint exercises, we have also leveraged RED FLAG for large force employment focused on

driving integration in a world-class warfighting training environment. For our offensive forces presenting global strike capability, we walked slowly from niche *demonstrations* to combat force rehearsals of concepts. Our next step is to harden these relationships to improve our readiness, and ability to put effects on target.

---

---

This operations culture shift  
is our greatest challenge and  
holds the promise to be our  
greatest force multiplier.

### ***Don't skimp on the process***

In addition to shifting our language, cyber operations have also started to use joint and air-minded processes to assess risk and respond to incidents. The rigor used by aircraft safety boards following an aircraft incident has been ported to cyber. When incidents occur across the cyber terrain, we no longer simply consider them a 'technological glitch'; cyber incidents have direct impacts on missions and therefore some require the establishment of an Operational Review Board to assess causes, capture key lessons, and drive improvements.

Another example of our focus on operationalizing the cyber culture is the application of the PBED (Plan-Brief-Execute-Debrief) process to previously 'standard patching' processes. With the establishment of a common cyber enterprise, small changes can have global effects. Therefore, our cyber forces now follow a rigorous process to plan, brief, execute, and debrief the implementation of AF-wide change requests, tasking orders, defensive upgrades, and other activities. The focus is on operational outcomes and continuous improvement.


### ***Looking to the future***

Our Air Force cyber forces are more capable than ever before, and continue to improve every day. Our continued focus on operational cyber forces ensure DoD networks are



better defended, Combatant and Air Component Commanders are receiving more of the critical cyber effects they require, and our nation's critical infrastructure is more secure. Collectively, we should all be tremendously proud of the progress made.

That said, culture is one of the most difficult thing to change. We have made great strides inculcating a cyber operations culture within AFCYBER (24 AF), but our Air Force's reliance on cyber expands far beyond our units. A culture of air-minded cyber operations must be entrenched in every Airman, from our senior leaders to new Airmen graduating from technical training school.

Driving this operations culture shift is our greatest challenge and holds the promise to be our greatest AF-wide operations force multiplier if we are successful. Time is the culprit. In no period in history have we witnessed the pace of threats increase with such speed, sophistication or proliferation. Our pace of learning and adapting continues to accelerate, and we are confident our collective innovation and drive will enable mission success. It is why our AFCYBER (24AF) vision is to be the *World's Preeminent Cyber Force ... Powered by Airmen, Fueled by Innovation.* 

## NOTES

1. D. Hayden, Air-Mindedness. Air and Space Power Journal, 2008. Retrieved from <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj08/win08/hayden.html>

# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆



# Cyber Situational Awareness

---

Major General Earl D. Matthews (USAF, Ret)

Dr. Harold J. Arata III

Mr. Brian L. Hale

## INTRODUCTION

Cyberspace threats are real and growing. Worldwide cybersecurity trends and implications support these assertions: 97% of organizations analyzed in 63 countries have experienced a cyber breach; 98% of applications tested across 15 countries were vulnerable; in 2014, threat groups were present on a victim's network a median of 205 days before detection; \$7.7M was the mean annualized cost of cyber crime across 252 global, benchmarked organizations in 2015; and 60% of enterprises globally spend more time and money on reactive measures versus proactive risk management.<sup>[1][2][3][4][5]</sup> "Every conflict in the world has a cyber dimension," testified ADM Michael Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency, before the House Armed Services Committee in March 2015.<sup>[6]</sup> These facts, and the increasing acknowledgement regarding the importance of cyberspace on operations, place organizational leaders under immense pressure to make sound cybersecurity investment choices. Cybersecurity has truly become a political, military, economic, social, information, infrastructure, physical environment, and time concern for senior leaders.

The emergent and dynamic characteristics of cyberspace are a result of rapid advancements in computer and communication technologies, as well as the tight coupling of the cyberspace domain to physical operations. Military organizations have embedded cyberspace assets (information technology) into their mission processes as a means to increase operational efficiency, improve decision-making quality, and shorten the sensor-to-shooter cycle.<sup>[7]</sup> This cyberspace asset-to-mission dependency can place an organization's mission at risk when a cyberspace incident (e.g., the loss or manipulation of a critical information resource) occurs.

Non-military organizations typically address this type of cybersecurity risk through



Major General Earl D. Matthews (USAF, Ret) is Vice President of Hewlett Packard Enterprise's Enterprise Security Solutions Group for HPE Enterprise Services, U.S. Public Sector. In this role, General Matthews leads a team of cybersecurity experts who deliver strategic, end-to-end solutions to help HPE clients anticipate, overcome, and reduce security threats and vulnerabilities while achieving their missions. Earl Matthews is a highly decorated, award-winning retired Major General with a successful career influencing the development and application of cybersecurity and information management technology. Throughout his three-decade military career, General Matthews held many key assignments, including cyber operations, plans and policy, resource and budget management, acquisitions and staff positions.



Dr. Harold J. Arata III is the Executive for Cybersecurity Strategy at Hewlett Packard Enterprise, Enterprise Security Solutions. In this role, Dr. Arata is a key adviser to C-Suite level executives on cybersecurity strategy formulation. Prior to his arrival at Hewlett Packard Enterprise, Dr. Arata was a not-for-profit scientific research institute Cyber Center Director and was the Director-U.S. Air Force Cyberspace Technical Center of Excellence educating 650 joint cyber professionals a year. He also served as a Senior Military Professor, Air Force Institute of Technology, conducting defense-focused research at the Master's and Ph.D. levels. Preceding Dr. Arata's federal civil service, he was an active duty 2-year below-the-zone select to Full Colonel. Dr. Arata's military awards include being individually designated Best-in-Air Force as the Lt Gen Leo Marquez Communications-Electronics award winner and the Legion of Merit.



Mr. Brian L. Hale is the Associate Director for Cybersecurity Strategy at Hewlett Packard Enterprise, Enterprise Services, U.S. Public Sector, Enterprise Security Solutions. Prior to his arrival at Hewlett Packard Enterprise, Mr. Hale was the Operations Officer for a Cyber Center of Excellence at a not-for-profit scientific research institute. Preceding his career in industry, Mr. Hale was appointed as the Deputy Chief, Cyber Professional Continuing Education Division, Air Force Cyberspace Technical Center of Excellence, Air Force Institute of Technology (AFIT). Mr. Hale also served in the U.S. Air Force and retired in April 2012 after a 26-year career. Mr. Hale earned a Master of Science Degree in Information Resource Management from the AFIT, a Bachelor of Science Degree in Management/Computer Information Systems from Park University, and two associate degrees.

an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so an economical set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level. The explicit valuation of information and cyber resources, in terms of their ability to support the organizational mission, enables the creation of a continuity of operations plan and an incident recovery plan.

While this type of planning has proven successful in static environments, military missions typically involve dynamically changing, time-sensitive, complex, coordinated operations and tasks involving multiple organizational entities. The relationship between missions, operations (military action), and tasks are shown in Figure 1.

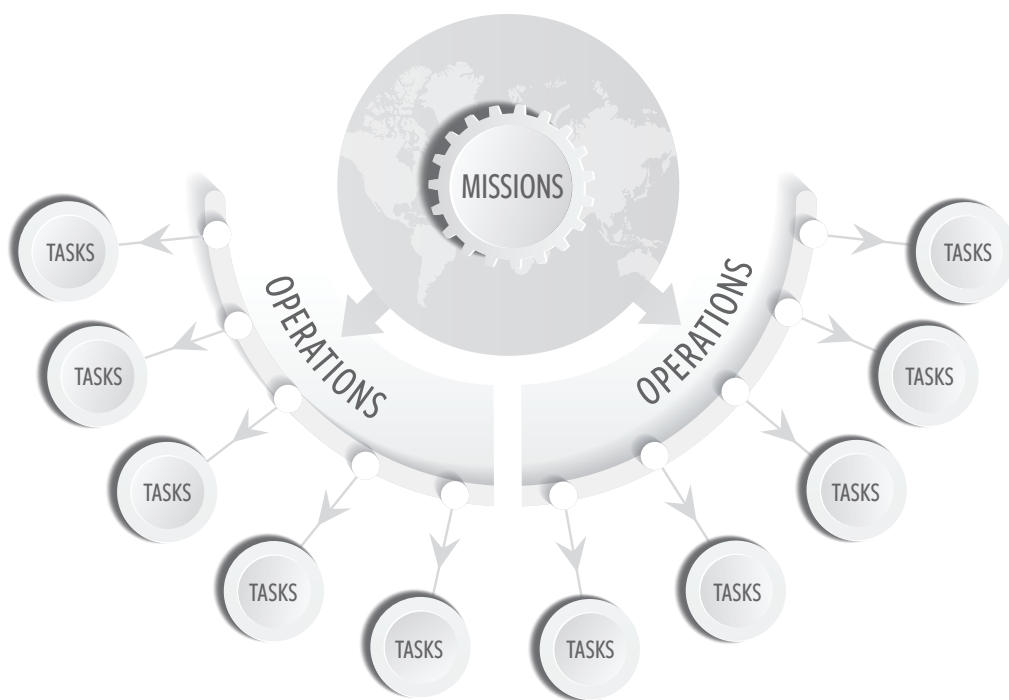


Figure 1. Relationship of missions, operations, and tasks

### ***Mission Assurance***

To assure a military organization's complex mission, several key steps must be accomplished; e.g., prioritizing mission essential functions, mapping mission dependencies on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.

It was once accepted that cybersecurity in an enterprise could only be achieved by driving out all vulnerabilities that are susceptible to exploitation. But, there is now increasing recognition this isn't necessarily the case or even possible. LTG Edward Cardon, Commanding General, U.S. Army Cyber Command, stated, "It's increasingly clear we can't protect everything."<sup>[8]</sup> Additionally, recent high-profile events in both the public and private sectors clearly demonstrate that like other threats—both natural and man-made—protecting every asset from every threat is futile and costly. As outlined in the most recent US Department of Defense (DoD) Cyber Strategy;

Leaders must take steps to mitigate cyber risks. Governments, companies, and organizations must carefully prioritize the systems and data that they need to protect, assess risks and hazards, and make prudent investments in cybersecurity and cyber defense capabilities to achieve their security goals and objectives. Behind these defense investments, organizations of every kind must build business continuity plans and be ready to operate in a degraded cyber environment where access to networks and data is uncertain. To mitigate risks in cyberspace requires a comprehensive strategy to counter and if necessary withstand disruptive and destructive attacks.<sup>[9]</sup>

Through a risk management program, operational risks may be eliminated or reduced to an acceptable level. However, given DoD hosts 7 million networked devices and

---

In 2014, 97% of organizations analyzed in 63 countries have experienced a cyber breach; 98% of applications tested across 15 countries were vulnerable.

15,000 network enclaves, and the DoD networks are probed thousands of times an hour with an ever increasing frequency and sophistication, it is likely impossible to reduce all cyberspace-related risks to zero or an acceptable level.<sup>[6][7]</sup> Rosenzweig (2009) noted even when it is feasible to eliminate

risk it may be impractical because the risks are systemic and resistant to traditional cost-benefit analysis. He continued, "in a world where the identity of the threat cannot be determined with confidence, mitigation of that threat is problematic."<sup>[10]</sup>

Acknowledging these challenges, as well as the difficulty of conducting risk management across an enterprise as large and complex as the DoD, a mission assurance strategy and processes, enabled by cyber situational awareness, must be employed (Figure 2).

Figure 2. Mission assurance strategy<sup>[1]</sup>

### ***Situational Awareness and Cyber Situational Awareness***

Moreover, to achieve any level of mission assurance and command and control confidence, Situational Awareness (SA) must be maximized so operational risks may be mitigated, managed, or resolved prior to a mission or during operations (reference Figure 2). SA is traditionally defined following the pioneering and influential work of Mica Ensley in 1988; SA is a long-studied field concerned with the perception of the surroundings and derivative implications critical to decision makers in complex, dynamic areas such as military command and security.<sup>[12]</sup>

Given the progressive and usefulness of SA research, SA is being applied to cyberspace. To this end, and in concurrence with Franke and Brynielsson (2014), cyber SA is posited to be a subset of SA.<sup>[13]</sup> Through a holistic SA approach, the combination of information from different disciplines, e.g., human intelligence, geospatial intelligence, and open source intelligence, can be combined with cyberspace sensor information (e.g., intrusion detection system alerts) to enhance overall cyber SA. The concepts and strategy for achieving cyber SA requires disciplined processes, enabling technologies, and collaborative organizations.

### ***Wanted: New Thinking in Cybersecurity and Cyber SA***

While the sophistication of cyber threats facing governments and industry grows every day, traditional thinking about how cybersecurity leaders should fight that challenge is evolving. Longstanding assumptions and tired orthodoxies aside, cybersecurity and cyber SA means building new frameworks from the ground up to include reinventing an organizations ability to understand mission dependences and cyber threat landscapes,



reforming of training and cyberspace operator qualifications, as well as the refashioning of supporting network tools that enable an organization's personnel to operate at the speed of light—netspeed. Commanders recognize status-quo thinking and incremental change rarely keeps pace with an aggressive adversary.

Cyber SA can be a complex and bewildering topic for policy makers not used to working within the daily cyberspace ecosystem. However, by applying “well-recognized risk management principles commonly used in other security domains, such as transportation and port security, and comparing the approach to dealing with other predatory and adaptive threats, including terrorists and foreign intelligence services, a clearer picture emerges.”<sup>[14]</sup> What matters in transforming an organization's cyber SA is intelligence, integration, speed, analytics, expertise, and resiliency (Table 1). Simply stated, no single countermeasure is effective against every threat. Resourcing cybersecurity and cyber SA becomes a matter of sound risk management decisions, based on threats and vulnerabilities to data, applications, systems, and networks that have the highest likelihood of impacting mission assurance.

Table 1. What matters in transforming your cyber SA mission space

<b>Intelligence Matters</b>	Rely on up-to-the-minute threat intelligence to proactively understand threats to your cyber SA enterprise. Achieved through actionable threat research and commercial threat intelligence sensor grid and network analysis.
<b>Integration Matters</b>	Automated synthesis of SA monitoring information from across your enterprise infrastructure, operational and intelligence processes, and applications. Achieved through integrating data flows into a continuous monitoring platform.
<b>Speed Matters</b>	Breaches are inevitable; cyber SA assessments, automation, and analytics reduce reaction time and mitigate damage to your enterprise. Achieved through innovative analytics.
<b>Analytics Matters</b>	Ingest data to analyze, correlate, and visualize events to produce actionable, contextual, scalable, and insightful cyber SA. Achieved through analytics platforms that leverage devices and their data as assets, moving organizations from being reactive to proactive across their operations.
<b>Expertise Matters</b>	Leverage industry cyber SA expertise to help better understand vulnerabilities, manage threats, and achieve mission assurance. Achieved through support, managed services, training, and education.
<b>Resiliency Matters</b>	Be prepared for the unexpected by protecting your data confidentiality, integrity, and availability. Cyber SA achieved through end-to-end data protections, virtualization, and continuity plans.

An escalating number of industry insiders believe more creative thinking, more research, more knowledge management and more SA—not just more technology—is needed. Dr. Thomas Homer-Dixon outlined just such an ingenuity gap, “in general, as the human-made and natural systems we depend upon become more complex, and as our demands on them increase, the institutions and technologies we use to manage them must become more complex too, which further boosts our need for ingenuity. The crush of information in our everyday lives is shortening our attention span, limiting the time we have to reflect.”<sup>[15]</sup> It is these increasing demands, combined with today’s greater network complexity, and rising social unpredictability, that make it more critical than ever that smart technical and social solutions be ready at a moment’s notice. The MIT scientist Edward Lorenz’s Chaos theory is also used to describe how small changes can lead to widely varying results and path dependence.<sup>[16]</sup> As such, it is essential to leverage a new cyber SA model that incorporates the aforementioned: intelligence, integration, speed, analytics, expertise, and resiliency.

For example, the new cyber SA model may include leveraging industry threat intelligence feeds and analysis integrating millions of sensors, with the capability to analyze billions of files, web objects and flows per day, while continuously sharing those results within the organization and

externally with its’ partners. The benefits of commercial intelligence feeds are overwhelming, both qualitatively and quantitatively, compared to today’s military sensor collections. Additionally, there is a reluctance by many organizational partners to share intelligence data due to their sources and methods. Michael Daniel, the White House cybersecurity coordinator, described information sharing as “critical to effective cybersecurity,” and the Cybersecurity Act of 2015 was passed in December 2015 to provision this information sharing.<sup>[17][18]</sup>

Cybersecurity has traditionally worked from a defensive position, supported by an industry whose default mode is to patch, prevent, block and build *improved* versions of the same technology. This innovation deficit on the part of the industry has impacted end users, military commanders, chief information officers, and chief information and security officers who are trying to build mission assurance security strategies against unprecedented threat levels. A great number of organizations still have a security strategy that was formulated when the concepts of intelligence, integration, speed, analytics, expertise, and resiliency were not fully understood. With President Obama’s recent call for a 30-day sprint in July of 2015 to improve government-wide cybersecurity perfor-

---

---

No single countermeasure is effective against every threat. Cybersecurity and cyber SA becomes a matter of sound risk management decisions.

mance after the Office of Personnel Management compromise, cybersecurity experts believe it is “unlikely agencies can solve in a month a problem that’s been festering below the radar for years.”<sup>[19]</sup> Alan Paller, Director of SANS Institute, stated, “If you come back in a few months, you will see that the change has slowed radically because OMB [Office of Management and Budget] will go on to other metrics.”<sup>[20]</sup> Organizations need to step-up with accelerated, sustained, and measured cybersecurity efforts.

For example, most public sector requirements and requirements processing, which is a 2-to-10 year cycle, has to accelerate in support of a rapid cyber acquisition model that can keep pace with the quantum leap in technology advances from year-to-year. Furthermore, a typical 5-year DoD Future Years Defense Program (FYDP) planning and budgeting cycle is not rapid, considering advances in cyberspace technologies consistently double every 2-3 years when put in the context of observations of Moore’s and Bezos’ laws (Figure 3).

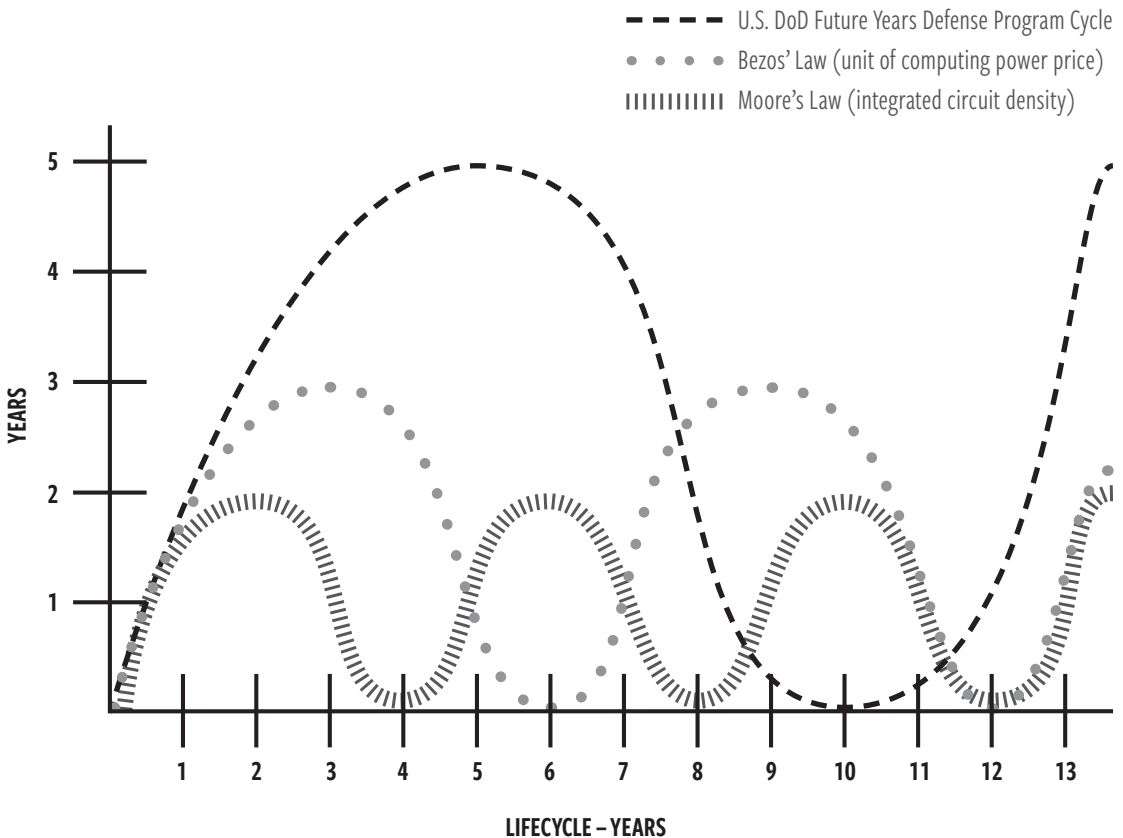


Figure 3. Comparison between rapid technology developments and the requirements capability document FYDP process

Looking ahead, technology continues to enhance mission capabilities in numerous ways, and with that comes the critical challenge of maintaining cybersecurity throughout on-going missions, operations, and tasks. However, with increased cooperation and innovative thinking, a thorough understanding of the imminent cyberspace threats to mission assurance may be achieved.

Through an effective cyber SA lifecycle, like the proposed framework in Figure 4, any organization can further enhance mission assurance by improving the timeliness, relevance of notification, and incident response following a cyberspace incident. Moreover, a cyber SA warning capability may prevent a cyberspace incident from occurring.

A cyber SA framework defines appropriate security metrics, security enforcement policies, controls and technologies, security management, operations workflow, and multi-level risk management reporting dashboards that can fuse and address these and many more complex issues facing current organizations both in the private and public sectors.

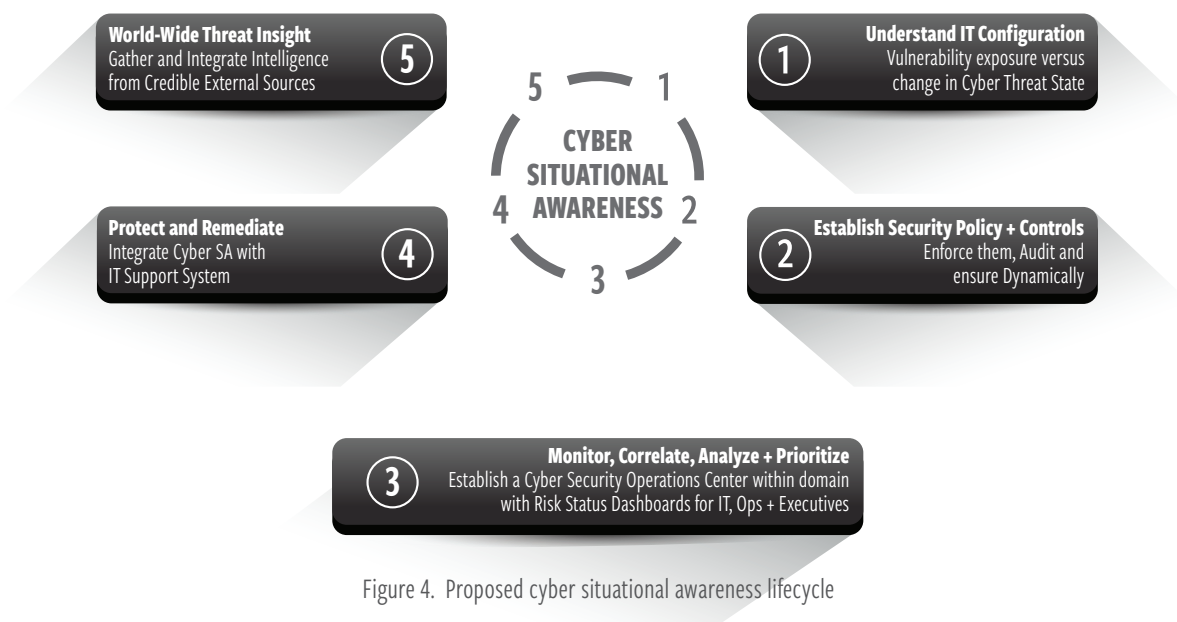


Figure 4. Proposed cyber situational awareness lifecycle

## CONCLUSION


Protecting enterprise networks and providing mission assurance without a significant cyber SA and warning capability will continue to be a challenging mission. Without cyber SA, a fragmented, imperfect view into enterprise networks and how cyber assets map to tasks, objectives, and missions occurs. This incomplete view thwarts threat detection, trend analysis, and preemptive actions creating slow or non-existent reactions to threats and changing conditions thereby constricting a senior leader's decision-making space.

Cyber SA for most enterprises are presently disjointed, rudimentary, ad hoc, too focused on technical analysis, lacking important cyber threat intelligence data feeds from supporting providers, and missing actionable, contextual analytics. Moreover, personnel are currently delivering very limited strategic cyber SA capabilities for senior leadership. This flawed view can be operationally blinding to any organization.

Initial progress has been made today by many organizations to increase their cyber SA capability, for example, with the implementation of security operations centers. However, most organizations may further strengthen their cyber SA and warning capability by incorporating commercial cyber threat intelligence capabilities, bolstering their cyber SA structures, implementing a comprehensive cyber workforce education and certification program, fusing cyber SA data into actionable information (tactical, operational, and strategic dashboards), and recognizing cyberspace as a domain. By weaving an enabled mission assurance strategy with an empowered cyber SA construct is a high return on investment for any organization operating in today's high threat environment.

The time has arrived for a new model, more ingenuity, and recognizing the importance of cyber SA in defense of an organization's enterprise. What matters in transforming an organization's cyber SA is intelligence, integration, speed, analytics, expertise, and resiliency. Enacting just such a cyber SA framework can and will enable an organization to more effectively protect itself both today and into its' future.

### ***Timeless Senior Leader Insights***

Dave Packard, one of Hewlett-Packard founders, stated, "It is necessary that people work together in unison toward common objectives and avoid working at cross purposes at all levels if the ultimate in efficiency and achievement is to be obtained."<sup>[21]</sup> This is part of Hewlett Packard Enterprise's core company objectives and shared values: transform to a hybrid infrastructure; protect your digital enterprise; enable workplace productivity; empower the data-driven organization. Hewlett Packard Enterprise believes this is especially the case for enhancing cybersecurity and cyber SA. Success will depend on a common effort by all stakeholders. Hewlett Packard Enterprise is committed to working with legislators, agencies, clients and citizens to achieve this most important objective. 

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

## NOTES

1. FireEye and Mandiant, A FireEye Company. *Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model*. Retrieved from <http://www2.fireeye.com/rs/fireeye/images/fireeye-real-world-assessment.pdf>. (accessed 2015).
2. Trustwave. *Trustwave Global Security Report*. Retrieved from [https://www2.trustwave.com/rs/815-RFM-693/images/2015\\_TrustwaveGlobalSecurityReport.pdf](https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf). (accessed 2015).
3. Mandiant, A FireEye Company. *M-Trends 2015: A view from the front lines*. Retrieved from <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf>. (accessed 2015).
4. Ponemon Institute, & Hewlett Packard Enterprise. 2015 *Cost of Cyber Crime Study: Global*. Retrieved from <http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/> (accessed October, 2015).
5. Hewlett Packard Enterprise. *Protecting your business with a more mature IT security strategy*. Retrieved from <http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA5-5744ENN.pdf>. (accessed November, 2015).
6. Pellerin, C. CYBERCOM Chief: Cyber Threats Blur Roles, Relationships. *DoD News*. Retrieved from <http://www.defense.gov/News-Article-View/Article/604225> (accessed March 6, 2015).
7. National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems*. NIST Special Publication 800-34, Revision 1. (Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, 2010).
8. Cardon, Edward, Lt. Gen. Cyber can't protect everything. *Signal, Armed Forces Communications Electronics Association*. Retrieved from <http://www.afcea.org/content/?q=cyber-cant-protect-everything> (accessed 2014).
9. Carter, A. *The DoD Cyber Strategy*. Retrieved from [http://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf). (accessed April 17, 2015).
10. Rosenzweig, P. *National Security Threats in Cyberspace—Post Workshop Report*. Retrieved from [http://www.abanet.org/natsecurity/threats\\_%20in\\_cyberspace.pdf](http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf) (accessed 2009).
11. Alberts, C.J. & Dorofee, A.J. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments*. Carnegie Mellon University Networked Systems Survivability Program Report CMU/SEI-2005-TN-032, 2005.
12. Endsley, M. R. Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (SAGE Publications Vol. 32, No. 2, 1988) 97-101.
13. Franke, U., & Brynielsson, J. Cyber situational awareness—a systematic review of the literature. (*Computers & Security*, 2014) 46, 18-31.
14. Hewlett Packard Enterprise. *National Cybersecurity State Policy Leadership Managing risk in the Cyber World*, (Hewlett Packard Business White Paper, 2012) 3.
15. Dixon, H. *The ingenuity gap, How can we solve the problems of the future?* (New York, NY: Knopf Publishing, 2000).
16. Lorenz, E. *Predictability: Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas?* 1972 Retrieved from [http://eaps4.mit.edu/research/Lorenz/Butterfly\\_1972.pdf](http://eaps4.mit.edu/research/Lorenz/Butterfly_1972.pdf).
17. Fischer, E. *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*; Congressional Research Service CRS Report R42114. Retrieved from <https://www.fas.org/srg/crs/natsec/R42114.pdf>. (accessed 2015).
18. Consolidated Appropriations Act of 2016, H.R.2029, 114th Congress. Retrieved from <https://www.congress.gov/bill/114th-congress/house-bill/2029> (accessed 2015).
19. Golden, H. *Security Experts Point to OPM's Biggest Cybersecurity Failure*. Retrieved from <http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/> (accessed July 21, 2015).
20. O'Connell, M. *Where do agencies go now post-cyber sprint?* Retrieved from <http://federalnewsradio.com/cybersecurity/2015/08/agencies-go-now-post-cyber-sprint/> (accessed August 4, 2015).
21. Packard, D. *HP Corporate Objectives and Shared Values*. 1957 <http://www.hp.com/hpinfo/about/hp/values-objectives>.



# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆





# Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age

---

Dr. Chris C. Demchak

## ABSTRACT

Cyberspace is becoming bordered and moving away from westernized civil society control. Governments and major organizations are building a “Cyber Westphalia” of bordered national jurisdictions, forming in pieces across nations. Furthermore, the world has entered into the era of ‘cybered conflict’ among states and non-state organizations. As the centers of economic and demographic power move to Asia, rising non-westernized states are contesting the western notions of an unbordered, civil society led global cyberspace directly, as well as inevitably western control of the rest of the international economic system. That the challenge happened in less than a generation is, in large part, due to these western societies whose key actors were captured by a tri-part convergence during the formative ‘frontier era’ of cyberspace. Three cognitive frames guided western approaches to the growing global substrate: unrealistic optimism in early utopian cyber visions, security-blind IT capital goods business models, and western societies’ deeply institutionalized hubris about the permanency and moral superiority of their Cold War legacy control of the international system. Time is running out for scholars and practitioners to consider, debate, and consense on alternatives that can rescue some remnant of the free and open cyberspace created by the West for its own tolerant cultural preferences, transparent legal regimes, and comparative well-being.

“Taking away developing countries’ ability to control public opinion through Internet controls and surveillance would result not in more openness, but instead in *blood* and *hatred*.”

September speech by Hao YeLi, Vice Chair, China Institute for Innovation Development Strategy, former senior officer PLA General Staff. (Mozur 2015)



With engineering, economics, and comparative complex organization theory/political science degrees, Dr. Chris C. Demchak is the RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College. In her research on cyberspace as a globally shared insecure complex 'substrate', Demchak takes a systemic approach to emergent structures, comparative institutional evolution, adversaries' use of systemic cybered tools, virtual worlds/gaming for operationalized organizational learning, and designing systemic resilience against imposed surprise. Recent works include *Designing Resilience* (2010, co-edited); *Wars of Disruption and Resilience* (2011); and a draft manuscript entitled *Cyber Westphalia: Cyberspace's Redefining International Economics, Conflict, and Global Structures*.

### *Rising Cyber Westphalia*

Today, the early halcyon 'frontier era' of cyberspace is over, and its visions have failed. It is not, as the early cyber prophets envisioned—an automatically benign global 'village' open to all, free or nearly free of cost or technological restrictions or borders or governments, uniformly positive in its effects, and automatically democratizing for any citizen or nation that used it. (Rheingold 1993) Cyberspace is becoming bordered and moving away from westernized civil society control.

Over the past twenty-five years of cyberspace's formative 'frontier era', global digitization created a worldwide socio-technical economic system (STES)<sup>[1]</sup> that serves now as a key substrate underlying and connecting the key functions of all digitizing societies. It did not, however, convert political systems or cultural preferences to the civil society ideals embedded deeply in western democratic government, commercial, and civil society approaches to the global internet.<sup>[2]</sup> Rather than a universally equitable and unfettered prosperity and democracy spreading globally, the open internet imposed on western nations unprecedented economic losses as cyber-enabled criminal transnational organizations (TNOs) and free riders exploited the open, poorly secured global networks. (PWC 2014) Furthermore governments, their proxies, witting fellow travelers, and criminal or activist opportunists adopted global cybercrime's exploit tools and demonstrated techniques to compete with, spy on, disrupt, undermine, and over time debilitate their perceived adversaries. (Riley and Vance 2011)

Instead of the nirvana of no governments and free prosperity, governments and major organizations are building cyber defenses, a "Cyber Westphalia"<sup>[3]</sup> of bordered national jurisdictions is forming in pieces across nations. As this formative era ends,

the world has entered into the era of ‘cybered conflict’<sup>[4]</sup> among states and non-state organizations. As the centers of economic and demographic power are moving to Asia, rising non-westernized states are not simply quietly folding into the existing liberal economic international system as presumed. Rather, led by China in particular, they are less and less likely to ‘blindly ape’ democratic civil society rules of law. (Peerenboom 2006) They are contesting the western notions of an unbordered, civil society led global cyberspace directly, as well as the inevitability of western control of the rest of the international economic system. (Chen 2001) The rise of these cyber borders coupled with cybered conflict and a growing non-western rejection of western civil society values dramatically reduces the chances that the coming international economic system of the cybered world will reflect the future envisioned by the western democracies who created cyberspace.

Why did western societies lose purchase on the key early formative period of the emerging global structure and the likely imperatives of the future deeply cyber world? While not successful in practice, the early cyber-prophet visions did nonetheless succeed in deeply defining the basic “deep institution”<sup>[5]</sup> presumptions that framed twenty years

---

## Cyberspace is becoming bordered and moving away from westernized civil society control.

of policy objectives in the western democratic civil society’s public and private organizations. While declining in their overt expression, the effects of their cognitive framing continue to symbol-

ically and practically distract the key westernized communities from recognizing quite different trends across the international system.<sup>[6]</sup> Eventually the global system would have altered as a rising China and the other ninety percent of the world’s population outside of Europe, the US and their democratic allies modernized. (Nye Jr 2011) However, without cyberspace’s open connectivity to both legal and illegal sources of wealth and power-enhancing knowledge, this sea change might have been more gradual, taking three or four generations to truly challenge existing presumptions. Western societies’ complacency, however, helped this challenge emerge so quickly by not reacting to accept some—and redirect other—trends as the cyberspace substrate changed underlying interactions and perceptions of interest.

This article argues that three cognitive blinders in western approaches operated over this formative era to hinder accurate assessments of emerging reality: unrealistic optimism in early utopian cyber visions, security-blind IT capital goods business models, and western societies’ deeply institutionalized hubris about the permanency and moral superiority of their Cold War legacy control of the international system. The ‘winners’ of the Cold War ignored the reality of their own cultural uniqueness, of the lack of security

concerns for national wealth in their own IT capital goods manufacturing, and of the possibility that the international system created in the Cold War could ever be contested and bested by rising adversaries. A different future is emerging—a crisis-ridden, conflictual, uncivil and post-western Cyber Westphalia.

### ***Optimistic Visions and Naively Insecure Designs***

The original internet's design, its optimistic visions, its globalized access to national riches, and its civil society norms are products of the dominance of the civil societies such as the US during the Cold War. Civil society control over the globe's rules of exchange was never inevitable, not permanent, but it was seen as both by the West's policy makers, strategic thinkers, and most academics. Improperly understood was the uniqueness of the first 40 years since the end of World War II, during which time the major peer adversaries—China and Russia—helpfully self-isolated economically. That absence made it possible for the US without too much bloodshed or costs to install and maintain the West's preferences across the international system.<sup>[7]</sup>

By the middle of the 1990s, after forty years, that system did look to be permanent as former outside states such as Russia and China seemed to be complying more or less. For those creating the visions of the early internet, it was easy to assume nothing else would happen when a communication tool built for western cultural norms and legal enforcement regimes spread to considerably different communications, values, and political systems. (Goldsmith and Wu 2006) Since WWII, other cultures complied; they did not contest—at least not successfully. The technical designers of the original internet were focused on the intellectual challenge of networks and the reliability of transmission—not on security or other cultures. The libertarian commercial entrepreneurs creating the early IT capital goods industry focused on the domestic first before moving to the international markets—assuming both were legally assured by the apparent permanence of the western liberal international economic system. (Feldmann 2010)

### ***Enduring Optimism and Presumptions***

After almost three decades of development by US government financial support to universities, cyberspace emerged for public and commercial use about twenty-five years ago as the 'internet'. (Hafner 1999) It was already embedded with the ideology of a public good. Sharing the technological developments and access openly across universities, it became a social presumption embedded as an intrinsic and inevitable requirement for the generation of new ideas, languages, and software. Security was an afterthought, in large part because the time-consuming, fault-intolerant coding languages used by academics were hard to hack in any case, and the early networks connected to relatively few and well known small communities.<sup>[8]</sup> Furthermore, concerns were limited because early cyberspace did not uniformly connect everything important, and the biggest threats were unreliable

transmission, some cybercrime, and possibly sociopathic organizing. (Rochlin 1997) The bigger concern was just getting the sharing to be reliably transmitted. (Kinnersley 2015).

By the mid-1990s, as the internet spread with this presumption of free sharing and

---

---

Over the past 25 years of cyberspace's formative 'frontier era', global digitization created a worldwide socio-technical economic system.

access, the new 'cyberspace' acquired almost mystical properties—despite it being completely a man-made, -owned, -maintained, -updated, -monitored, and deployed 'peer-or-pay' underlying substrate.<sup>[9]</sup> Barlow's 1996 "Declaration of Independence for Cyberspace" declared all networked individuals to be 'netizens' beyond the reach of

governments. Not by declaration or any necessary act by those individuals, but by simply entering into this connected world of such complexity and connectedness that no bureaucracy could succeed in controlling it, netizens thus freed themselves of any legacy societal constraints. (Barlow 1996) Otherwise-credible scholars said it would produce a world in which laws emerge from the collective consciousness without governments or national boundaries. That vision became deeply embedded and continues to be subconsciously endorsed today as a basic framing—that this new digitized world village would be inevitably a universally benign, freely shared, implicitly democratic global space for good, uplifting all who connected into it.<sup>[10]</sup> (Norris and Jones 1998)

### ***Commercialization of Flawed Basic Design for Speedy Marketing***

Converging with this vision of a new free world of ideas and collective virtual freedom was an oversized set of promises about economic prosperity from the e-commerce and IT capital goods industries. The utopian vision merged with the libertarian view that the Internet and all of its technological designs and development were something that governments and borders should never touch. (Rosenzweig 1998) The threat was that, if the regulators were allowed to inhibit the freedom of the web, its prosperity—even its generativity—would be lost.<sup>[11]</sup>

As the computer industry fed the emerging internet frenzy through the 1990s, however, commercial interests were—unlike their academic colleagues—both impatient and proprietary. (McCarthy 1978) By the early 1990s, the demand from the private sector to fund and therefore use these network tools for commercial purposes was overwhelming. The National Science Foundation, the last official guardian of the otherwise publicly sponsored internet, opened it up to private carriers. (Frischmann 2001) From then on, the influence of commercialization on the dominant design of the web was profound. Those more secure academic languages which took too long and too many resources for commercial returns

were displaced.<sup>[12]</sup> (Trickey 1988) Funding flowed to those computer scientists migrating from the earlier languages known to be intolerant of mistakes in code, such as the LISP (1960s on), to those that could tolerate mistakes in code and yet perform their intended tasks, such as C+ (1990s on). (Wexelblat 2014) With the rise of commercial interests, entrepreneurs such as Bill Gates wanted a healthy return on his software investment. He did not want to make sure programs were perfect before selling them—DOS stands for ‘Dirty Operating System’—nor to have code shared widely before a return on investment could be achieved. (Rosenzweig 1998)

The result was a commercialization tsunami with an IT capital goods business model that emphasized the rapid factory-like production<sup>[13]</sup> of standardized, fault-tolerant (more easily hacked) software getting to the market as quickly as possible.<sup>[14]</sup> (Houidi and Pouyllau 2012) Beyond login passwords to keep account ownership clear, security concerns were still chiefly reliability of performance, safety of transmission of bytes, and design efficiencies in production for the emerging markets across the US and Europe. (Anderson 1994)

So dominant was this perception of the libertarian IT capital goods business model as benign and uniformly economically advancing that it migrated into the taken-for-granted presumptions of the cyber utopian communities as well. With both communities coming to view the open internet’s economic benefits as explicitly tied to a lack of government controls for any reason, these communities came to view erecting national jurisdictions across cyberspace as economically daft as well as morally unacceptable in this new cybered world.<sup>[15]</sup> (Lessig 2004/original 1998) Until as recently as 2011, those in the open internet community still dismissed evidence of bits and pieces of cyber national borders emerging unstoppably across cyberspace.<sup>[16]</sup> (Betz and Stevens 2011)

### ***Predation at Global Scale Prompts a National Searches for Bolt-On or Keep-Out Options***

Rather than democracy and ubiquitous prosperity, the rapidly coded, more easily hacked languages which dominated exchange and hardware across the open, insecure cyberspace enabled the rise of transnational predators en masse. This now freely available, insecure, global substrate offered small and large bad actors three major nearly free advantages never available in history to anyone other than emperors or superpowers—open access to large scale in organizations, to globally close proximity, and to unprecedented levels of precision in remote operations.<sup>[17]</sup> A massive underground global cybercrime market developed with specialized submarkets, warranties, and tools including services. (Glenny 2011) Governments and transnational criminal organizations soon joined into the global hacking for information, money, and political or economic leverage.<sup>[18]</sup> A dizzying variety of predators and adversaries for a wide range of reasons—including ‘because we can’—now threaten any open and digitally advanced nation’s entire inventory of critical largescale ‘socio-technical-economic systems’ (STESs) and—in the process—the nation’s long-term economic vitality.<sup>[19]</sup>



Even what was once the remaining superpower—the United States—found it did not have the resources to simply absorb or repel the daily onslaught of attacks by state and non-state actors.<sup>[20]</sup> Major corporations began recognizing—and finally admitting—major information losses. Some, such as Canada’s Nortel, went bankrupt after theft of their critical intellectual property.<sup>[21]</sup> After only two years in office as the Director of the National Security Agency, General Keith Alexander in 2012, called

---

The utopian vision merged with the libertarian view that the Internet and all of its technological designs and development were something that governments and borders should never touch.

the losses in intellectual property and future market returns “the greatest transfer of wealth in human history.” (Paganini 2013) The Netherlands discovered in 2012, that its 2010 GDP growth had been halved by the costs of cybersecurity, and the market losses associated with the massive intrusions.

According to a recent PWC report for 2014, given the World Bank’s estimate that the entire globe’s GDP totaled \$75 trillion in 2013, then the losses of trade secrets and therefore future earnings could range as high as \$2.2 trillion. The effects are concentrated so far in westernized nations, shaving as much as 1% to 3% off a nation’s annual GDP. (PWC 2014)

### ***Cyber Westphalia Rising Unwitting in the West and Eagerly in the East***

Borders rise for many reasons, but largely for reasons of security—i.e., increasing certainty about averting losses from nature or adversaries.<sup>[22]</sup> As the cyber extractions from victim nations have mounted dramatically, so have the cyber defenses in bits and pieces across nations. (Deibert and Crete-Nishihata 2012) The great threats to economic vitality and nationally critical infrastructure via cyberspace now offer adversaries the potential to cripple the modern state over time while avoiding traditional kinetic war. While the foreign policy language still strongly endorses and calls for a globally free and open internet, the domestic policy language of concern by westernized government has risen from cybercrime, to critical infrastructure protection, and to losses to the entire economy over time, with cyber security now labeled a tier 1 threat.<sup>[23]</sup> Even nations known for their civil society, Sweden for example, have taken steps domestically to monitor<sup>[24]</sup> what enters or leaves their national territories networks. The intent is security—to use that information if needed to protect citizens, enforce the laws, or ensure the nation’s critical functions.<sup>[25]</sup>

Yet the symbolic visions of the cyber libertarian and the commercial power of the IT capital goods communities continue to dominate in collective opposition to legitimizing



national borders in cyberspace. (Kroker and Kroker 1996) This rejection endures for a third and most embedded reason—the deeply institutionalized western sense that democracy is the inevitable end state of all societies. (Wrobel 2013) Borders in the internet are unnecessary and immoral—as well as generally wastefully futile—impediments to achieving that global end state. (Atkinson and Brake 2015)

### ***China's Sovereignty Narrative and Western Hubris***

“America spreads the ideas of democracy widely across the world, but in cyberspace, it’s the opposite,” [Hao YeLi, former PLA senior official 2015] said. “The United States continuously maintains a system to monitor the rest of the world but asks other countries to strictly control themselves and remain within bounds. This unsymmetrical line of thinking continues.” (Mozur 2015)

China wants her borders in cyberspace and will take nothing less. (Gresh 2008) Yet an unacknowledged western hubris—a supreme confidence in the moral and economic superiority of the western approach to society and cyberspace, however, leads governments and civil society promoters to consistently refuse to accommodate the Chinese sovereignty demand. They routinely conflate civil society cyber societies with economic success, despite China's rise having already demonstrated to the rest of the world that the two could be separated successfully.<sup>[26]</sup> (Kalathil and Boas 2010) Furthermore, China is not alone. The Chinese model of societal information control and their wider neo-capitalist business practice preferences have a powerful resonance with the rest of the non-westernized world. (Chen 2001)

Since entering the global web in the 1990s, China’s spokespersons have consistently made its sovereignty expectation explicit—including across the internet. (Whiting 1996) China’s leaders had relatively good reasons to expect a campaign to alter the global narrative to accept simply national sovereignty in cyberspace would be successful. (Qiu 1999) China was developing the economic weight to muster forces internationally and bilaterally against this western dismissal of their demand for cyber sovereignty. This campaign focused on using the influence and visibility of particular major institutions in the current international system.<sup>[27]</sup> (Yong and Pauly 2013) Given the Cold War history, the leaders of China, Russia, and many other non-westernized leader could reasonably have expected that sovereign rights of a nation would be upheld for cyberspace. (Duara 1997) Unlike space, for example, it is completely a man-made underlying substrate relying mostly on undersea cables connecting one nation’s sovereign soil to another.<sup>[28]</sup> (Blum 2013) Furthermore, the United Nations is a foundation of the post-WWII liberal international system and its basic multilateral character has been reinforced by the international system’s decisions strictly upholding sovereignty, even while led by the United States. China’s strategists may be forgiven for not recognizing what they faced in the opposition. If one was not taken with the optimism visions, swayed by the economic libertarianism, or imbued with a western

superiority hubris, expecting sovereignty would be more or less automatic is a reasonable opening position.

By 2011, China's leaders had taken a decade to position themselves and some allies in key influential positions in international technical organizations, and across critical IT and related markets. However, achieving an endorsement of cyber sovereignty by the international community did not emerge. Rather, the prestigious 2011 GCCS 'London Process' international internet governance meeting, for example, once again endorsed open Internet as a human right inside every nation. For the Chinese, these western internet governance blind spots do seem to reflect a cybered form of the deafness of imperialists.<sup>[29]</sup> Furthermore, the civil society promoters have moved the terms of the debate in order to build another obstacle to acknowledging the primacy of national cyber sovereignty. Internet governance conferences—not sponsored by China, close allies, or the UN—now elevate the moral and efficacy value of 'multistakeholder' meetings—involving states, commercial interests, and civil society groups in governance—as equal to or better than the 'multilateral' state level meetings traditionally held by the UN.<sup>[30]</sup>

In the last four years, Chinese senior political and corporate leaders have moved to an even more aggressive use of rising economic power<sup>[31]</sup> with an openly wider agenda. The new wider narrative uses the rise of China as a future great or super power to rationalize its right to question the current international system's governors. (Li and Shaw 2014) Not only is China determined to ensure its own national sovereignty in cyberspace and in other sectors, but also they now overtly challenge the western dominance of global Internet governance system as a whole. The apparent objective is to influence changes in cyber-

---

---

Even nations known for their civil society—Sweden for example—have taken steps domestically to monitor what enters or leaves their national territories' networks.

a period of roughly 70 years because of its demographic and economic weight in the global system. (Liu and Deng 2010) With its poorly secured global pathways across poor and wealthy national socio-technical-economic systems, cyberspace shortened that transition dramatically—to fifteen to twenty years. (Drezner 2004) China's public and commercial leaders and thinkers now see an opportunity to advance more quickly and are moving to seize the opening.

Moving to alter cyberspace's international realities has proven illuminating for China.

space producing a structure more convenient, or at least less threatening, to Chinese national preferences (DeNardis 2014) In the 1980s, the former leader of China Deng Xiaoping predicted China would equal the US as a global great power over

For example, its meteoric economic rise may have been funded in good part by its cyber business knowledge and data extractions; however, China's political and economic leaders have learned to exploit the impunity benefits and 'teflon' legitimacy of a near superpower with a very large attractive internal market. (Rowley 2010) The unclassified 2013 Mandiant report empirically leaves little doubt that an aggressive Chinese military unit (among others) has been one key source of the massive cyber data extractions. (Mandiant 2013) Yet very little punitive action has been publicly announced in international fora, in markets, or bilaterally as corrections on China for these activities emanating from its territory. In 2000, China was allowed to enter the World Trade Organization (WTO) due to its size and despite its inability to meet the basic WTO obligations. (Blancher and Rumbaugh 2004) By 2014, however these requirements have never been met, and yet there is no discussion of ejecting China. (Atkinson and Ezell 2015) Rather, by 2015 the US President and China's President Xi signed an agreement on cybercrime and data extractions that has no mechanisms for enforcement. (Hvistendahl 2015) This level of agreement, and the general tolerance of poor behavior internationally, constitute the kind of accommodations made between peer great powers, an inference that Chinese media has noted. (Hao 2015)<sup>[32]</sup> Indeed, despite signing the 2015 agreement to curb cybered exploitations of information for commercial benefit, the evidence is that Chinese hackers continued at the same pace during and after the fall signing, although the composition of the 'usual suspects' changed.<sup>[33]</sup>

Furthermore, while China's narrative on cyber borders seems to fall on deaf ears in western states' foreign policy circles, by 2015 cyber borders in praxis are being grudgingly and indirectly accepted. A wide variety of Western documents, including the widespread rise of national cyber security strategies, recognize a government's obligation to protect their own national cyber jurisdictions.<sup>[34]</sup> As the Chinese have argued, each bilateral agreement that acknowledges the responsibilities of another state in the parts of cyberspace connecting within their established national territory is one that in effect acknowledges the existence of national cyber jurisdictions. (Rowley 2010; Liu and Deng 2010) From the practical perspective of developing nations' leaders for whom the Chinese firm Huawei is building—for the national telecommunications public agency—4G networks for nearly no upfront costs, opposing borders in cyberspace conflicts with the rising reality. (Gagliardone 2015) (Chung and Mascitelli 2014)

Building on the opening provided in its fight for national cyber sovereignty, China now routinely uses its own version of a 'globally noble' argument to collect allies—that the whole of the internet does not serve the equity and rights of all nations. (Bhuiyan 2014) In response to the publicly explicit western expectation that cyberspace under civil society will democratize a society, the Chinese narrative accentuates the instability and greater dissent that can accrue with a border-spanning open internet. (Cui and Wu 2016) This dissent can prove unhealthy for authoritarian or semi-governed states and their leaders,

and the argument can produce allies despite apparent geostrategic differences. In 2011, Russia joined China in proposing an “International Code of Conduct for Information Security”. Despite the document’s resounding rejection by the West, its language formally expresses the basic desire for absolute sovereignty to be the governing principle of the international cybered system. (Farnsworth 2011) Left open is how this fully bordered cyberspace is to be governed internationally. However, the Chinese narrative in speeches and publications then connects this essential element, state cyber sovereignty, with a world where China rises to its proper place as the first great power that is benignly ‘non-hegemonic’. The term is used to mean no state including China as a rising world power will tell any other state how to operate internally, thus neatly eliminating the US as the old style global internet hegemon with its civil society preferences from the center of the global international system’s governance. (Kivimäki 2014)

China has moved fast from its frustrations with the West on cyber sovereignty to more aggressively seizing on the international influence openings offered by a hegemon and allies apparently unable or unwilling to bribe or bully China and allies into

---

---

By 2015, President Obama and China’s President Xi signed an agreement on cybercrime and data extractions that has no mechanisms for enforcement.

compliance. While not eager for military confrontation, conflicts with the US on economic, information, institutional, and cultural fronts have been expected by China’s pragmatists for some time, seen as an inevitable outcome when a current hegemon resists being displaced. (Liu 2015) (Zhao 2015) In the past few years,

China’s new leader Xi Jinping and official media outlets have increasingly openly rejected civil society ‘western’ values—chief among them freedom of speech, and more aggressively asserted the downsides of continuing US web dominance. (Kemp 2015) The Chinese narrative has hardened publicly against the combination of cyber utopian vision, libertarian economics, and westernized civil society hubris. (Zheng and Lye 2015). While much in cyberspace is classified in western nations, the battlefield for this narrative is not. In response, many internet governance-related forums: GFCE, IGF, Global Commission on Internet Governance, NETmundial Initiative, WSIS, WCIT, and the GCCS ‘London Process’ have signaled a redoubling rather than weakening of western pressure for China’s acquiescence to UN human rights applied to cyberspace internally as part of the future cybered world system.<sup>[35]</sup> Tensions are deepening across cyberspace.

### ***Cybered Conflict and Rising Post-western Cyber Westphalia***

Not only has the West lost purchase on whether national borders (re:jurisdictions) are

erected in cyberspace, its three collective cognitive failures: vision, business model, and hubris have also encouraged the conditions for cybered conflict as these borders rise. With the western actors increasingly accusing China of a myriad of cybercrime and other violations of civil society laws and expectations, China's response is to deny accusations, and accuse in return. China also uses the full weight of its demographic and economic power, by fair means and foul<sup>[36]</sup> across a range of overt and covert activities, to change the perceptions of potential allies about their own economic and societal interests versus supporting US cast as the failed hegemon of the internet. (Karatzogianni 2010) With the two major nations at loggerheads over governance and pride of first place, the Cyber Westphalian system rises around them; highly conflictual in cybered terms, and possibly also in kinetic terms on occasion.

Cybered conflict is two, or more, faced. While its lack of overt violence encourages system versus system conflict to remain generally short of traditional kinetic war, the deceptiveness in tools and opaqueness of originators inherent to its operations undermine existing conflict-dampening institutions, tropes, and norms. (Goldsmith 2013) On one hand, China's cyber forces, volunteers, and proxies can do a great deal to make it harder for westernized actors to persuade, bribe, or bully enough other states to truly consolidate enforceable international rules against sovereignty or ensure democratic human rights. In a deeply cybered world, options abound from cybered conflict's three advantages in scale, proximity, and precision for conducting long running, below physical conflict, global campaign through social media,<sup>[37]</sup> largescale economic extractions, and increasingly sophisticated international mercantilism. (USCESRC 2014) (Perlroth 2013) Also available are multiple avenues by which to individually bribe or bully, including blackmail or intimidation, others in major or allied nations' positions to work against the West's role and its allied unity across a wide variety of international venues, especially those dealing with global governance of cyberspace. (Shakarian et al. 2013)

On the other hand, cybered conflict's mechanisms and tools are largely developed by the international cybercrime community not under any state's credible control as yet. Furthermore, these criminals' excesses, many from China, are what majorly drives the westernized states to build national borders unwillingly or unwillingly despite the foreign-policy positions. The massive economic losses have alerted the western security and political leaders to the kinds of behaviors associated with cybercrime, cybered conflict, and even China itself. This economic loss recognition has crystallized a public divide between China with its pro-sovereignty allies, and the western consolidated democracies. (Lindsay 2013) For example, the US and its allies walked out of a heavily pro-sovereignty 2012 WCIT meeting hosted by the UN's ITU, which is increasingly influenced by China, recognizing they were going to lose a major vote. (Huston 2012) That collective demonstration of strong displeasure is unusual for western states. However, when such behavior is conducted by those who thought their preferences ruled the international system, it

suggests strongly that the changes China hopes to see may not be quietly accepted. (Jardine et al. 2015)

Cybered conflict also encourages misperceptions particularly due to the wide variation in the number of state and nonstate actors, and events that could be engaged at any given moment. Just as the West has continually got it wrong and set up the conditions for this conflict so rapidly, so too can China misperceive how far is risky in pushing for more than simply cyber sovereignty. While the US sees its efforts as benignly trying to help a peaceful rise of China into democracy, the Chinese elites view the western anti-border and civil society efforts as either inexplicably stupid, or an indication of a larger more threatening plan. (Gardner 2015) As they act and western security institutions respond, a wide variety of connected critical systems are being employed in this contest across cybered nations and complex systems. The greater the number of actors involved, the more surprise and misjudgment are encouraged. The two main adversaries routinely mis-

---

---

The massive economic losses have alerted the western security and political leaders to the kinds of behaviors associated with cyber-crime, cybered conflict, and even China itself.

perceive each other. The US sees itself as simply defending a universal good in an open global Internet by still rejecting borders and calling for universal civil society values. On the other hand, a cyber-emboldened China presents itself is merely trying to be sovereign as it develops. It is also hoping to hurry along

the hegemon's apparent decline with narratives, money, and stealth, and yet control the narrative of a no-threat peaceful rise well enough to stay short of physical conflict. Across a global and highly insecure underlying substrate, however, a plethora of other actors and systems actively, unwittingly, or unwillingly also have multiple options at low cost to enter the struggle and muddle the indicators and conditions that both the US and China perceive. In pursuing what seems a golden opening to shorten the path to the global top rank, China's leaders and their allies could easily misjudge the level of quiescence the western powers will exhibit as their utopian, libertarian, and hubris-borne presumptions fail to deliver.

As trends stand today, the deeply interconnected mass of national socio-technical economic systems will increasingly reflect the preferences of more authoritarian states in the emergent center of economic power in Asia. (Berger 2015) Chinese business practices, in particular, are personalistic, social clan based, affective, opaque, and quite variant from the western economic world of legal protections and transparent, enforced contracts. (McDonald 2012) Without a compensating balance in economic and political weight by



the small number of states that are consolidated democratic civil societies, such things as common liberal technological standards, transparency in currency stability, and open, nonarbitrary rule of law support for international commercial contracts and IP will slowly migrate to reflect the routinely nontransparent Asian—specifically Chinese—business as preferences, along with internet governance structures. (Bu and Roy 2015) (Hannas et al. 2013)

China's thinkers increasingly discuss how the West, specifically the US, might respond as the failing hegemon, and, to be fair, some form of this cybered competition between the US and China would have emerged anyway. However, without the distraction of a vision, the economic libertarian push, and the border and values insults energizing a rising adversary, cybered conflict is likely to have emerged more slowly with differently weighted advantages. The delay would have better encouraged western democratic public and commercial leaders to recognize the negative global trends and to find more studied, grounded, and feasible paths in adapting to differing global power distributions. China's leaders would still have believed that their population weight in the world entitles their rise to be one of two great powers in the world at some point in the future. Cyberspace's vulnerabilities would still have made hacking for profit into opportunities to level the playing field in securing China's rise, but these opportunities do not make it urgent to move more quickly. When the current internet hegemon and its allies constantly seem to threaten the fundamentals of China's political system, then it does become less tolerable for China to wait until the 2049 date (or later) anticipated by Deng Xiaoping for this rise of China to be settled.

---

The US sees itself as simply defending a universal good in an open global Internet by still rejecting borders and calling for universal civil society values.

Still, China might have moved more circumspectly, had the discovery of the massive losses in economic wealth produced firm reactions by the West—ones that would be more likely to be interpreted in China as worthy of a strong hegemon. In recent years, China strategic and economic actors have overcome their surprise at how little the West, specifically the US, has done publicly about the economic violations, other than repeated calls for civil society norms and meetings. Many Chinese publications now openly assume the apparently quite rapid decline of the US as a hegemon as mere segue to addressing the urgent need for China to take the opportunity to accelerate its rise.<sup>[38]</sup>

This Internet governance challenge to civil society presumptions is only the beginning of a host of looming multi-domain contests more likely to be lost in the future if the West is unable to recognize and alter the cognitive framing created in the early frontier era of

cyberspace. It has been costly for the western democracies to be so distracted. Chances to slow this rise of cybered conflict have been squandered across a range of missed technological transformation, societal resilience, markets reform, and informed policy opportunities. Even if western national leaders abruptly announced acceptance of a global system of national cyber sovereignties, the civil society narrative now has a major, well-funded, covertly reinforced, and overtly well promoted counter-narrative about the rules governing the future cybered world led by more authoritarian sensibilities. To be blunt, there are no guarantees of dominance—or even a future world filled with democracies—for the consolidated democratic civil societies who are less than ten percent of the globe’s population.<sup>[39]</sup> In any era, it is tough to cement allies if one is seen to be in decline. In the near to far term, there is no clear path by which these western economies could support the level of Cold War enforcement efforts ensuring the world would follow their lead.

The liberal international economic system cannot survive long on its own, save possibly in name only without its wealthy western civil society governors and enforcers. Nonwestern cultures indifferent to civil society values were not offered much of a middle ground in the western vision of the global cyberspace, not even the option to be sovereign within their own networks. Now China and Russia, among others, offer that sovereignty as a minimum in their alternate narrative, along with political models that can seem more likely to be stable internally than democracy, and yet, economically advancing.<sup>[40]</sup> Indeed, Ringmar (2012) offers the proposition that given differences in power sources, use of emotions in foreign policymaking, and the over reliance on the vagaries of socially mediated public opinion formation, the two quite different international systems in history (Sino-centric or the Tokugawa Japan) may prove better adapted than the Westphalian system to the kinds of conflict and social organizing needed in the coming deeply cybered and conflictual century. (Ringmar 2012) This notion may be extraordinarily offensive to those imbued with the dominant triumphalism of western democracies, but not to the other ninety percent of the globe’s population likely to be led by the practices, preferences, and products of China and Asia for most of the rest of this century.

Forcing the future global cyberspace to keep to the western model of an open internet transiting into and across all nations is normatively desirable, but it is no longer possible. Needed urgently is a feasible alternative structure for a conflictual cybered world—one that is markedly less than global, less than normatively preferred, and less consumed with globalizing western libertarian economics. It must be one that accepts the rise of cyber sovereignty among nations which will not in the foreseeable future be civil societies—if ever. Yet this alternative must preserve some remnant of the free and open cyberspace created by the West for its own tolerant cultural preferences, transparent legal regimes, and comparative well-being. This honest conversation and critical research about the future of the international socio-technical-economic system needs to begin now.<sup>[41]</sup> The



alternative is to eventually concede to a global version of China's 'info-web' internet. (Schneider 2015) The conflictual and eventually post-western cyber Westphalian international system is rising very fast indeed. 🛡️

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

## BIBLIOGRAPHY

- Anderson, Ross J. 1994. "Liability and computer security: Nine principles." In *Computer Security—ESORICS 94*: Springer.
- Atkinson, Robert, and Doug Brake. 2015. "Net Gains: A Pro-Growth Digital Agenda." *Democracy* (36):9.
- Atkinson, Robert D., and Stephen Ezell. 2015. "False Promises: The Yawning Gap Between China's WTO Commitments and Practices." Washington DC: Information Technology and Innovation Foundation.
- Barlow, JP. 1996. "A Declaration of the Independence of Cyberspace." *Humanist - Buffalo* 56 (3):18-9.
- Barrett, Louise, S Peter Henzi, and David Lusseau. 2012. "Taking sociality seriously: the structure of multi-dimensional social networks as a source of information for individuals." *Philosophical Transactions of the Royal Society of London B: Biological Sciences* 367 (1599):2108-18.
- Barry, Jack Joseph. 2014. Don't Be Evil: Should Access to the Internet Be Conceptualized as an Instrumental Human Right? Paper read at American Political Science Association 2014 Annual Meeting Paper.
- Berger, Ron. 2015. "The transformation of Chinese business ethics in line with its emergence as a global economic leader." *Journal of Chinese Economic and Foreign Trade Studies* 8 (2):106-22.
- Betz, David J, and Tim Stevens. 2011. "Chapter two: Cyberspace and sovereignty." *Adelphi Series* 51 (424):55-74.
- Bhuiyan, Abu. 2014. *Internet governance and the global south: demand for a new framework*: Palgrave Macmillan.
- Blanchard, Jean-Marc F, and Norrin M Ripsman. 2008. "A political theory of economic statecraft." *Foreign Policy Analysis* 4 (4):371-98.
- Blancher, Mr Nicolas R, and Mr Thomas Rumbaugh. 2004. "IMF: China - international trade and WTO accession." International Monetary Fund.
- Blum, Andrew. 2013. *Tubes: A Journey to the Center of the Internet*: HarperCollins Publishers.
- Blumler, Jay G, and Stephen Coleman. 2001. *Realising democracy online: A civic commons in cyberspace*. Vol. 2: IPPR London.
- Bradley, James. 2015. *The China Mirage*. New York: Little, Brown and Company.
- Brink, Gustav Francois. 2013. "Anti-dumping and China: three major Chinese victories in dispute resolution."
- Bu, Nailin, and Jean-Paul Roy. 2015. "Guanxi Practice and Quality: A Comparative Analysis of Chinese Managers' Business-to-Business and Business-to-Government Ties." *Management and Organization Review* 11 (02):263-87.
- Cerf, Vinton G. 2012. "Internet access is not a human right." *New York Times* 4:25-6.
- Chen, Ming-Jer. 2001. *Inside Chinese business: A guide for managers worldwide*. Cambridge, MA: Harvard Business Press.
- Chung, Mona, and Bruno Mascitelli. 2014. "Huawei's Battle: Cold War or Commercial War?" *Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations*:107.
- Clark, David. 2010. "Fighting over the Future of the Internet." *IEEE Internet Computing* 10:22-3.
- Cui, Di, and Fang Wu. 2016. "Moral goodness and social orderliness: An analysis of the official media discourse about Internet governance in China." *Telecommunications Policy* 40 (2-3):265-76.
- Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*: McClelland & Stewart.
- Deibert, Ronald J, and Masashi Crete-Nishihata. 2012. "Global governance and the spread of cyberspace controls." *Global Governance: A Review of Multilateralism and International Organizations* 18 (3):339-61.
- Demchak, Chris C. 2012. "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World." In *Securing Cyberspace: A New Domain for National Security*, ed. N. B. a. J. Price. Washington, DC: The Aspen Institute.

## BIBLIOGRAPHY

- . 2013. “Economic and Political Coercion and a Rising Cyber Westphalia.” In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, ed. K. Ziolkowski. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.
- Demchak, Chris C., and Peter J. Dombrowski. 2011. “Rise of a Cybered Westphalian Age” *Strategic Studies Quarterly* 5 (1):31-62.
- DeNardis, Laura. 2014. *The global war for internet governance*: Yale University Press.
- Diamond, Larry Jay. 1994. “Toward democratic consolidation.” *Journal of Democracy* 5 (3):4-17.
- Dombrowski, P. J., and C. C. Demchak. 2014. “Cyber Westphalia: Asserting State Prerogatives in Cyberspace.” *Georgetown Journal of International Affairs*, special issue on cyber.
- Duara, Prasenjit. 1997. “Transnationalism and the predicament of sovereignty: China, 1900-1945.” *The American Historical Review*:1030-51.
- Dunlap Jr, Charles J. 2001. “Law and military interventions: preserving humanitarian values in 21st century conflicts.” In *Humanitarian Challenges in Military Intervention Conference*, ed. K. S. o. G. Carr Center for Human Rights Policy, Harvard University. Washington, DC.
- Farnsworth, Timothy. 2011. “China and Russia Submit Cyber Proposal [“International code of conduct for information security”].” *Arms Control Today*:35-6.
- Feldmann, Anja. 2010. *The Internet Architecture-Is a Redesign Needed?*: Springer.
- Fountain, J. E. 2001. *Building the Virtual State: Information Technology and Institutional Change*: Brookings Institution Press.
- Friedman, George. 2010. *The next 100 years: a forecast for the 21st century*: Anchor.
- Frischmann, Brett. 2001. “Privatization and Commercialization of the Internet Infrastructure.” *Columbia Science and Technology Law Review* 2 (1):1-70.
- Gagliardone, Iginio. 2015. “China and the Shaping of African Information Societies.” *Africa and China: How Africans and Their Governments are Shaping Relations with China*:45.
- Gardner, Maggie. 2015. “Channeling Unilateralism.” *Harv. Int'l LJ* 56:297.
- Glenny, Misha. 2011. *Dark Market*. New York: Random House.
- Goldman, David. 2011. “The cost of cybercrime—The price tag on corporate data breaches is soaring: The rise in cyber-crime is costing hundreds of billions of dollars each year.” *CNNMoney.com*, July 22.
- Goldsmith, Jack. 2013. “How cyber changes the laws of war.” *European Journal of International Law* 24 (1):129-38.
- Goldsmith, Jack L, and Tim Wu. 2006. *Who controls the Internet?: illusions of a borderless world*. Vol. 89: Oxford University Press New York.
- Goodin, Dan. 2010. “IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled.” *El Register*, January 14.
- Gorman, Siobhan. 2012. “Chinese hackers suspected in long-term Nortel breach.” *The Wall Street Journal*, February 14.
- Grant, Tim. 2014. On the Military Geography of Cyberspace. Paper read at ICCWS2014-9th International Conference on Cyber Warfare & Security: ICCWS 2014.
- Greer, John N. 2010. “Square legal pegs in round cyber holes: The NSA, lawfulness, and the protection of privacy rights and civil liberties in cyberspace.” *J. Nat'l Sec. L. & Pol'y* 4:139-54.
- Hafner, K. 1999. *Where Wizards Stay Up Late: The Origins of the Internet*: Simon and Schuster.

## **BIBLIOGRAPHY**

- Hannas, William C, James Mulvenon, and Anna B Puglisi. 2013. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*: Routledge.
- Hao, Qi. 2015. "China Debates the 'New Type of Great Power Relations'." *The Chinese Journal of International Politics* 8 (4):349-70.
- Hill, Richard. 2014. *Internet governance: the last gasp of colonialism, or imperialism by other means?*: Springer.
- Hughes, Kristin Ashburst. 1996. "Copyright in Cyberspace: A Survey of National Policy Proposals for On-line Service Provider Copyright Liability and an Argument for International Harmonization." *Am. UJ Int'l L. & Pol'y* 11:1027.
- Huston, Geoff. 2012. "Calling Stumps at WCIT: Win, Lose or Draw?" In *The ISP Column*. <http://wattle.rand.apnic.net/ispcol/2012-12/stumps.pdf>.
- Hvistendahl, Mara. 2015. "Not guilty as charged." *Science* 350 (6262):732-5.
- Irion, Kristina. 2009. "Privacy and security International communications surveillance." *Communications of the ACM* 52 (2):26-8.
- Jardine, Eric, Samantha Bradshaw, Dr DeNardis, Fen Osler Hampson, and Mark Raymond. 2015. "The Emergence of Contention in Global Internet Governance (Rpt 17)." In *Global Commission on Internet Governance (CIGI)*. London: Chatham House.
- Juuso, Anna Maija, Ari Takanen, and Kati Kittilä. 2013. Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs). Paper read at Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013.
- Kalathil, Shanthi, and Taylor C Boas. 2010. *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Washington DC: Carnegie Endowment.
- Karatzogianni, Athina. 2010. "The Thorny Triangle: Cyber Conflict, Business and the Sino-American relationship in the global system." *e-International Relations*. Online.
- Kayaoglu, Turan. 2010. "Westphalian Eurocentrism in international relations theory." *International Studies Review* 12 (2):193-217.
- Kemp, Ted. 2015. "China leaders oppose 'universal values,' but it may not matter: interview with Prof Steinfeld Brown University." *CNBC.com*, July 6.
- Keohane, Robert Owen, and Joseph S Nye. 1977. *Power and interdependence: World politics in transition*: Little, Brown Boston.
- Kinnersley, Bill. 2015. "A Chronology of Influential [computer] Languages, The [Computer] Language List: Collected Information On About 2500 Computer Languages, Past and Present." <http://people.ku.edu/~nkinners/LangList/Extras/langlist.htm>: University of Kansas.
- Kivimäki, Timo. 2014. "Soft power and global governance with Chinese characteristics." *The Chinese Journal of International Politics* 7 (4):421-47.
- Kopetz, Hermann. 2011. "Internet of things." In *Real-time Systems*, ed. H. Kopetz: Springer.
- Kroker, Arthur, and Marilouise Kroker. 1996. "Code Warriors." *CTheory.net*:2-7.
- Langheinrich, M. 2001. "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems." *LECTURE NOTES IN COMPUTER SCIENCE*:273-91.
- Lessig, Lawrence. 2004(1998 original). "The laws of cyberspace." In *Readings in cyberethics*, ed. R. A. Spinello and H. T. Tavani. Sudbury, MA: Jones and Bartlett Learning.
- Lewis, James, Lara Crouch, and Anastasia Mark. 2015. "Cybersecurity in Asia and the Role of US Leadership: an Interview with James Lewis." *Georgetown Journal of Asian Affairs* online <https://repository.library.georgetown.edu/bitstream/handle/10822/761158/GJAA%202.1%20Lewis,%20James.pdf?sequence=1&isAllowed=y>.

## BIBLIOGRAPHY

- Li, Xing, and Timothy M Shaw. 2014. "Same Bed, Different Dreams" and "Riding Tiger" Dilemmas: China's Rise and International Relations/Political Economy." *Journal of Chinese Political Science* 19 (1):69-93.
- Lindsay, David F. 2013. "What Do the XXX Disputes Tell Us About Internet Governance? ICANN's Legitimacy Deficit in Context." *Telecommunications Journal of Australia* online 63 (3):<http://doi.org/10.7790/tja.v63i3.432> (link is external).
- Liu, Jianhua, and Biao Deng. 2010. "America Hegemony: Is It To Decline or To Continue." *Pacific Journal* 1:1-8.
- Liu, Mingfu. 2015. *The China Dream: Great Power Thinking & Strategic Posture in the Post-American Era*.
- Mandiant, APT. 2013. "APT1 Report: Exposing One of China's Cyber Espionage Units (Feb. 2013)". [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).
- McConnell, Mike, Michael Chertoff, and William Lynn. 2012. "China's Cyber Thievery Is National Policy—And Must Be Challenged." *The Wall Street Journal*.
- McDonald, Paul. 2012. "Confucian foundations to leadership: a study of Chinese business leaders across Greater China and South-East Asia." *Asia Pacific Business Review* 18 (4):465-87.
- Mozur, Paul. 2015. "Chinese Official Faults U.S. Internet Security Policy [Ms. Hao YeLi]." *New York Times*, September 29.
- Nakashima, Ellen. 2013. "US Target of Massive Cyber-Espionage Campaign." *Washington Post*.
- . 2015. "Following U.S. indictments, China shifts commercial hacking away from military PLA to civilian agency MSS." *Washington Post*, November 30.
- Norris, Pippa, and David Jones. 1998. "Virtual democracy." *Harvard International Journal of Press Politics* 3:1-4.
- Norton-Taylor, Richard. 2010. "The UK is under threat of cyber attack, the national security strategy says- Home secretary outlines priority threats facing Britain ahead of the publication of the national security strategy today." *Guardian Online*, October 18.
- Nye Jr, JS. 2011. *The Future of Power in the 21st Century*. Cambridge, MA: Public Affairs.
- Oyedemi, Toks. 2014. "Internet access as citizen's right? Citizenship in the digital age." *Citizenship Studies*:1-15.
- Paganini, Pierluigi. 2013. "Cyber-espionage: The greatest transfer of wealth in history." *H+ Magazine online*, March 01.
- Peerenboom, Randall. 2006. "Law and development of constitutional democracy: Is China a problem case?" *The ANNALS of the American Academy of Political and Social Science* 603 (1):192-9.
- Perlroth, Nicole. 2013. "Hackers in China attacked The Times for last 4 months." *The New York Times*, January 30.
- Philpott, Daniel. 1999. "Westphalia, authority, and international society." *Political Studies* 47 (3):566-89.
- Pillsbury, Michael. 2015. *The hundred-year marathon: China's secret strategy to replace America as the global superpower*: Henry Holt and Company.
- Ponemon\_Institute. 2012. "Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles." <http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html> Hewlett Packard Research.
- PWC. 2014. "Global State of Information Security® Survey 2015." In *Annual State of Information Security Survey*. <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>: Price Waterhouse Cooper.
- Rheingold, H. 1993. *Virtual Communities: Homesteading on the Electronic Frontier*. Reading, UK: Addison Wesley.
- Richmond, Riva. 2011. "The RSA Hack: How They Did It." *New York Times*, April 2.
- Riley, Michael, and Ashlee Vance. 2011. "Cyber Weapons: The New Arms Race (The Pentagon, the IMF, Google, and others have been hacked. It's war out there, and a cyber-weapons industry is exploding to arm the combatants)." *Business Week*, July 20.

## BIBLIOGRAPHY

- Ringmar, Erik. 2012. "Performing international systems: two East-Asian alternatives to the Westphalian order." *International Organization* 66 (01):1-25.
- Rochlin, G. 1997. *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton: Princeton University Press.
- Rogers, Mike, and Dutch Ruppersberger. 2012. "Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A Report." Washington DC: US House of Representatives.
- Rosenzweig, Roy. 1998. "Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet." *American Historical Review*:1530-52.
- Rowley, Chris. 2010. "Commentary: China's chimera: miracle or mirage in the 'Middle Kingdom'?" *Asia Pacific Business Review* 16 (3):269-71.
- Scheinmann, Gabriel M, and Raphael S Cohen. 2012. "The Myth of 'Securing the Commons'." *The Washington Quarterly* 35 (1):115-28.
- Schneider, Florian. 2015. "China's 'info-web': How Beijing governs online political communication about Japan." *New Media & Society*:1-21.
- Schrage, Michael. 2011. "How Amazon or Apple Could Cause a War with China: Networked and cloud-based digital businesses are vulnerable targets for cross-border mischief that could cause international conflict, says Michael Schrage" *Harvard Business Review* online.
- Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. 2013. "The Dragon and the Computer: Why Intellectual Property Theft is Compatible with Chinese Cyber-Warfare Doctrine." In *Introduction to Cyber-Warfare: A Multidisciplinary Approach* ed. P. Shakarian, J. Shakarian and A. Ruef. New York: Syngres.
- Shih, Gerry. 2014. "Chinese Internet regulator welcomed at Facebook campus." *Reuters*, December 8.
- Shin, Henry. 2015. "The Relationship between the Arab Spring Revolutions and Entrepreneurial Inhibitors, Enablers, and Activity in North Africa." In *Comparative Case Studies on Entrepreneurship in Developed and Developing Countries*, ed. J. Ofori-Dankwa and K. Ormani-Antwi. Hershey, PA: IGI Global.
- Singer, Peter W, and Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*: Oxford University Press.
- Stewart, Susan. 2013. "Epilogue—From the 'colour revolutions' to the 'Arab spring': Implications for democracy promotion." In *Democracy Promotion and the 'Colour Revolutions'*, ed. S. Stewart. London: Routledge.
- Story, Louise. 2007. "Mattel Official Delivers an Apology in China" *New York Times*, September 22.
- Stuenkel, Oliver. 2013. "Rising Powers and the Future of Democracy Promotion: the case of Brazil and India." *Third World Quarterly* 34 (2):339-55.
- Trickey, Howard. 1988. "C++ versus Lisp: a case study." *ACM Sigplan Notices* 23 (2):9-18.
- Tully, Stephen. 2014. "A Human Right to Access the Internet? Problems and Prospects." *Human Rights Law Review*:ngu011.
- USCESRC. 2014. "2014 Annual Report to the US Congress." In *Annual Reports to the US Congress*, ed. U.-C. E. S. Commission. [http://www.uscc.gov/Annual\\_Reports/2014-annual-report-congress](http://www.uscc.gov/Annual_Reports/2014-annual-report-congress).
- Wexelblat, Richard L. 2014. *History of programming languages*: Academic Press.
- Whiting, Allen S. 1996. "The PLA and China's Threat Perceptions." *The China Quarterly* 146:596-615.
- Wrobel, David M. 2013. *Global West, American Frontier: Travel, Empire, and Exceptionalism from Manifest Destiny to the Great Depression*: UNM Press.
- Xu, Xueyang, Z Morley Mao, and J Alex Halderman. 2011. Internet censorship in China: Where does the filtering occur? Paper read at 12th Passive and Active Measurement Conference, May 20-21, at Atlanta, GA.

- Yong, Wang, and Louis Pauly. 2013. "Chinese IPE debates on (American) hegemony." *Review of International Political Economy* 20 (6):1165-88.
- Zhao, Suisheng. 2015. "Rethinking the Chinese World Order: the imperial cycle and the rise of China." *Journal of contemporary China* 24 (96):961-82.
- Zheng, Yongnian, and Liang Fook Lye. 2015. "China's Foreign Policy: The Unveiling of President Xi Jinping's Grand Strategy." *East Asian Policy* 7 (01):62-82.
- Zittrain, J. 2006. "A History of Online Gatekeeping." *Harvard Journal of Law & Technology* 19 (2):253-98.

## NOTES

1. This unprecedented and increasingly critical national-level connectivity and its effects requires expanding the well-established 'socio-technical systems' (STS) concept to reflect 'socio-technical-economic-systems (STES) undergirding the modern digitized society. The newer term is needed to spur a new generation of economic, societal, and interstate conflict theories designed for a cybered world of interpenetrating and conflictual national STESs. (Dombrowski and Demchak 2014)
2. The US developed a "free flow" doctrine as the basic tenet of US policy-making towards the internet. (Powers and Jablonski 2015) In Europe where it is not contested that commerce is regulated by governments, these ideals emphasized an 'unrestricted access' doctrine wherein citizens are completely free to access to the internet for social communications, as ensured as a moral obligation by governments. <http://eeas.europa.eu/policies/eu-cyber-security/>.
3. The "Westphalian" system began with the 1648 Peace of Westphalia treaty by which two neighboring European states agreed to the reciprocal recognition of consensually identified national borders. (Philpott 1999) The current and taken for granted permanency of these borders is profoundly a product of the Cold War era. (Kayaoglu 2010) See also (Demchak and Dombrowski 2011)
4. 'Cybered conflict' is unique to this emerging era in that it is a spectrum between peace and traditional war in which nations and transnational organizations use the deception in tools, opaqueness in originators with the three low cost offense advantages of scale, proximity, and precision to hinder each other's STESs in part or in whole, waxing and waning, and iterating according to the opportunities. Cybered conflict is a newer form of system versus system nonobvious conflict that is uniquely enabled by the insecure design of the global cyberspace. Cyberspace itself is not a 'commons' or increasingly even a 'shared resource' as envisioned by thinkers in the democratic societies. (Blumler and Coleman 2001) (Scheinmann and Cohen 2012) Rather, it is best viewed as a 'substrate' that spread under and penetrated up into every major society's critical functions, linking a wide variety of actors, critical processes, and wealth in unprecedented ways. (Demchak and Dombrowski 2011; Grant 2014) All conflicts of societal significance will be cybered henceforth. Few will be traditionally declared, kinetic, two nation struggles, making the national security tasks of democratic nations in particular much more challenging than any era since WWII. (Dombrowski and Demchak 2014)
5. Fountain argues that, once these notions become taken for granted as "deep institutions", it is extraordinarily difficult to get their adherents to recognize their binding power, let alone to change those barring highly unsettling events or long-term campaigns to wear down the usefulness of these notions for shared daily practices. (Fountain 2001)
6. A small but growing number of scholars and practitioners have publicly noted these deeply held presumptions. More recently, James Lewis of CSIS in Washington, a noted expert on cyber international relations, especially between the US and China, has reiterated with some frustration the enduring nature of these wildly optimistic, but rarely openly questioned presumptions. (Lewis et al. 2015) It must also be noted that a small handful of respected scholars supporting a globally open internet are clear-eyed about the true chances of achieving this normatively desirable outcome; they are to be applauded for their courage and persistence, and are not the target of this critique. In particular, works by Rob Deibert and his co-authors associated with the Munk Center, University of Toronto demonstrate this category. (Deibert 2013) They are, however, the exception overall.
7. Coercion is a staple of international politics and economics. The western powers after WWII certainly used the full range of fortunate circumstances, hard and soft power -- short of going back to war -- to achieve acceptably their goals for the international system. (Blanchard and Ripsman 2008) (Keohane and Nye 1977) Cyber coercion emphasizes deception in tools and opaqueness in originators across STESs and nations, making defense and public resistance difficult for the relatively transparent democratic nations. (Demchak 2013)
8. In 1995 and 1996 access to sites were shut down in Germany due to German laws on pornography and Nazi sympathizer materials. (Hughes 1996)



9. The problem of not knowing the basics about the global web continues, even among those charged with making highly consequential national policies. In 2011, at a senior level cyber policy conference, several senior US individuals offered deeply felt suggestions about governance of cyberspace. Later in the same conference, they confided to me that they did not know how the internet was actually constructed. (author personal observation) See also Singer and Friedman's 2014 book intended to try to compensate for this appalling ignorance. (Singer and Friedman 2014) The difficulty is that this and similar books are emerging now – twenty years on – after the developments outlined in this paper are already well advanced due in large measure to the early and widespread levels of ignorance about cyberspace as a socio-technical-economic system.
10. Arguments for access to wifi broadband as a basic human right equivalent to the right to existence are highly normative. (Tully 2014) (Oyedemi 2014) A variant argument is that access to ICTs is an 'instrumental' human right. (Barry 2014) See Cerf's cogent rebuttal. (Cerf 2012)
11. The embedded nature of this threat – the loss of economic innovation if the internet's libertarian path is disrupted-continues today, especially among the more technical thinkers and practitioners. For example, "if ISPs, diverge from the Internet tradition of the open neutral platform .... It might reduce the rate of innovation, reduce the supply of content and applications, and stall the internet's overall growth." (Clark 2010) For an interesting nuanced concern, Zittrain cautions against the loss of human gatekeepers able to balance both generativity and security, and the potential for the rise of regulators to dampen both in the name of meeting consumer calls for security. (Zittrain 2006)
12. The security of fault-intolerant languages such as LISP cost more in commercial production, while the fault-tolerant languages externalized such costs onto the using society. (Johnson 2005)
13. The phenomenon of employing a large number of young programmers to whisk out standardized code as fast as possible – with the plan to fix 'bugs' later -- was particularly attributed to Gates' Microsoft with its factory like cubicles and tasks of young programmers called 'Microserfs'. (Coupland 2004)
14. Often overlooked is the role of globalized mass production in enabling cyber predations in particular. The standardization so essential to the business model of major IT capital goods corporations such as Microsoft played a significant and role in the exceptional broad number of targets and elevated levels of economic losses to nations today. (Geer et al. 2003)
15. Buried in the thinking of even the more libertarian of scholars is that, while one must be left alone to use cyberspace as one likes, that use must nonetheless be standardized under open internet western rules. Clark for example argues for understanding of the developing world's "different governments with different cultures and rules and regulation, different users with different skills, ... onto which we will try to impose uniform Internet standards." (Clark 2010)
16. It is interesting to speculate whether, had this new world been content to stay under the regimes for which its legal and value presumptions were appropriate, the web might have remained within these states as a communally shared resource subject to reciprocal laws, conveyances, and mutually agreed upon limits to surveillance for privacy reason. (Langheinrich 2001)
17. For a longer discussion of these systemic advantages, see (Demchak 2012).
18. The global underground cybercrime black market is about 80% mid and low skilled actors who tickle with or use someone else's software program. The last 10-15% are the truly skilled coders – the 'wicked actors' – employed by states or transnational organizations and so good that they will get through most defenses. This group includes the so-called "Advanced Persistent Threats" (APTs) generally associated with espionage, but the wicked actor group is larger because of the transnational sources can be both focused on crime as well as espionage. (Demchak 2012) (Juuso et al. 2013) (Singer and Friedman 2014)
19. It is important to note how very recent is the realistic possibility of connecting every process to the internet and, thus, how disrupting to existing social systems. (Kopetz 2011)
20. (Richmond 2011; Schrage 2011) (Goodin 2010) (Ponemon\_Institute 2012; Goldman 2011)

21. The Nortel Corporations bankruptcy is a major and clear case of this kind of slow roll of national knowledge stocks. Nortel went bankrupt in 2009, having been exploited by the Chinese firm Huawei in 2006-2007 due to cyber extractions of critical data, and then beat to the broadband wifi market for which Nortel was preparing its major and existential launch. In 2010, the CTO of the former Nortel was publicly listed as working for Huawei and seeking small technology startups for Huawei 'investment'. (Gorman 2012) (Rogers and Ruppertsberger 2012) (Rogers and Ruppertsberger 2012)(Rogers and Ruppertsberger 2012) (Rogers and Ruppertsberger 2012) Hacking is increasingly so sophisticated that, despite the massive growth of the commercial cybersecurity industry, on average nearly a third of attacks penetrating into an organization are unstoppable. (Lumension 2015)
22. Human organizations were formed for certainty – i.e., critical 'foreknowledge' -- in gathering enough food and defending it, in keeping threats collectively at bay when sleeping, etc. In advanced nations, one tends to use the term security and forget that it really means certainty about a preferred outcome. To us, it seems strange that freed slaves would stay in place because the only certain meal or shelter was where they were, or that Egyptians having overthrown a dictator would shortly elect one of his cronies because they promised stability – i.e., certainty about what might happen the next day, which the Arab spring and freedom had not done. (Shin 2015) It is useful to remember this instinctive human reach for certainty buried deeply in national policies and choices. (Barrett et al. 2012)
23. The United Kingdom is arguably the first major westernized state to declare cyberspace threats to be in the top tier of national security threats. (Norton-Taylor 2010) The tier language has become a cross-Atlantic term of art indicating the level of importance a state attaches to defending itself in cyberspace.
24. It is important to note that filtering is not the same as monitoring. The former removes data access; the latter notes the data's movements and possibly the content. Another way to view the difference is to note that NSA has been accused of monitoring, while China is shown empirically to filter. (Greer 2010) (Xu et al. 2011)
25. The law assigning this mission and authority to the Swedish Federal Police passed in 2008. (Irion 2009)
26. Western hubris is deeply embedded in scholars regularly declare Chinese resistance to western preferences as transitory. (Peerenboom 2006) They have for over a century interpreted a wide variety of phenomena as indicators of progress towards the inevitable civil society model. (Bradley 2015)
27. The campaign includes exploiting the grey areas in western rules of law to benefit Chinese corporations or avoid punishment for infractions, a variant 'lawfare'. (Dunlap Jr 2001)(Brink 2013)
28. Many cyberspace policymakers, pundits, and civil society promoters do not really know the structural and contractual basics about the global web. Such folks are often resistant to discussing the physical aspects of technology, as though it did not matter for a largescale socio-technical-economic system such as cyberspace. Singer and Friedman's 2014 book was intended to try to compensate for this appalling ignorance. (Singer and Friedman 2014) The difficulty is that this and similar books are emerging now – twenty years on – after critical early perceptions and policy paths were already well advanced.
29. This inability to accommodate the concerns of developing – read 'lesser' – nations is of very long standing, not only in cyber issues. (Hill 2014) (Bhuiyan 2014).
30. The term 'multistakeholderism' is a term becoming widespread during the ICT driven globalization surge from the 1980s–mid 2000s began in the 1980s and surged dramatically in the 1990s through the 2000's. (Lund 2013) A strict read of democratic theory would find it odd that civil society activists would demand non-elected leaders of large corporations be given a seat in deciding the rules of interstate commerce, politics, cyberspace, and by extension, the tools of conflict. However, the key characteristic of the cyber utopian vision is its blending of individual freedoms with economic libertarian freedom and the presumption that a cybered world prosperity depends on both of them absolutely. (Calandro et al. 2013) For the IT capital goods industry, however, the borders and the values issues are not interlinked. The business models only require no governmental restrictions on products and no hindrances in access to all markets, not for example universal freedom of speech. Many major IT corporates concede to Chinese requirements for compliance in technological surveillance of Chinese citizens or in sharing proprietary code in order to maintain their access to the large Chinese markets. (Tan and Tan 2012) (Jiang 2012) (Shih 2014)

31. Aided by the western corporate and individual state genuflection before that wealth. In this 2007 story, a major US toy corporation is said to be forced to apologize for harming the reputation of China's manufacturers when those factories used lead paint in the toys they produced. The consequences for not apologizing was, and always is, the indirectly given threat of losing access to China's market. (Story 2007)
32. One piece characterizes the Chinese internet as having "ossified into a highly regulated yet profitable info-web". (Schneider 2015)
33. Interesting enough, while some analysts argued that China's People's Liberation Army (PLA) exploitation was declining over 2015, the Ministry of State Security (MSS) appears to have taken up the slack up to and through the signing as well. (Nakashima 2015) It is unclear what effect on Chinese cybered conflict hacking the massive 2015 OPM extraction of security data on over 23 million current and former US government employees will have. Digesting all that material could slow the development of operations as the unprecedented wealth of personal data offers Enigma-like intelligence opportunities, especially in extensive social engineering operations. The material will be used eventually. Employees can change passwords, but not their family history, dates of birth, etc.
34. The term 'consolidated' is used to distinguish a stable, functioning, modernized, democratic civil society from a developing nation recently civilianized, highly corrupt, prone to military coups, or ruled by a single party or strongman, yet which occasionally has what are generously called open elections and thus is labeled a democracy. (Diamond 1994)
35. These are, respectively, the Global Forum on Cyber Expertise, the Internet Governance Forum, World Summit on the Information Society, World Conference on International Telecommunications, Global Conference on Cyberspace, among many others.
36. A number of sources argue that the Chinese extraordinary economic advance from the rise of telecommunications giants such as Huawei and others has been fueled by stolen intellectual property, business intelligence, and rather well-established practices from bribery to blackmail. When whole proprietary products show up in massive production in China and then drive western producers out of business, Chinese rise merely through solid market performance is harder to prove. (McConnell et al. 2012) (Nakashima 2013) (USCESRC 2014; Hannas et al. 2013) (Hannas et al. 2013)
37. Russia's latest military doctrine explicitly includes as an integral part of modern warfare a total system battle, and the operational use of information weapons to create dissent in an adversary's nation. [https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C09\\_kle.pdf](https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C09_kle.pdf).
38. This hard turn in China's foreign behavior is palpable across a variety of areas from maritime demands to aggressive and dismissive behaviors in international conferences on internet governance. Long-term China observers have begun to publicly discuss their own wake-up moments in seeing a newly assertive China consciously and publicly rejecting the path to a democratic civil society. (Pillsbury 2015)
39. The role of India as a largescale nonwestern democracy in improving the odds for the long-term survival of democracies globally is woefully understudied. It is not included in this ten percent figure. (Stuenkel 2013)
40. It is a mistake to underestimate the negative demonstration effects on authoritarian or beleaguered political leaders when they consider the longer term consequences of a cyberspace-enabled Arab Spring-like dissent movement. (Stewart 2013)
41. Increasing the sense of surprise that could feed outrage and poorly considered policies is a US international relations literature largely is silent on adopting to the serious possibility of US decline, denies it, or bewails some aspect of it while calling for action to maintain the US's central role in the world. (Friedman 2010)

# Protecting the digitized society—the challenge of balancing surveillance and privacy

---

Dr. Janne Hagen

Dr. Olav Lysne

## ABSTRACT

**T**hrough technological development and the continuously expanding Internet, the challenges of physical distance, borders and time has diminished, enabling new and more efficient business models and concepts. With this technological development, however, follows an increase in global cybercrime, mass surveillance, internet censoring, and espionage. Terror attacks and cybercrime incidents are now forcing policy makers to balance surveillance and privacy through a paradox: While privacy regulations protect individuals' freedom of speech and safety from persecution, it may also restrain effective crime and terror investigation. In November 2015, the Norwegian Governmental Committee on Digital Vulnerability delivered an Official Norwegian Report (NOU) to the Minister of Justice and Public Security in which the problematic issue of balancing surveillance and privacy was emphasized. The intricate challenge is that in-between surveillance and the privacy lays the personal data—the new *gold* from a commercial perspective, a resource in the fight against terrorism from a security perspective, and a future threat of human rights from an individual perspective.

## 1. CYBER THREAT DEVELOPMENT IN RETROSPECT

Originally, the Internet was designed with the purpose of interconnecting a sparse network of selected trustees—it was not intended to be available to everyone. As time passed, protocols were developed and several networks of networks evolved, gradually merging into larger networks leading to an expansion that now serves everyone. Today, the Internet and the World Wide Web connects people and information around the world. However, with this expansion and dissemination of malware, security worries arose.



Dr. Janne Hagen holds a Master's degree in industrial economy and management. She received her PhD in information security in 2009. In 2008-2009 she was a visiting Fulbright Scholar at Naval Postgraduate School, Monterey, CA. From April 2015 she works at The Norwegian Water Resources and Energy Directorate (NVE) with SCADA and ICT security. She was until then working as principal scientist at the Norwegian Defence Research Establishment (FFI) and associate professor at the University of Stavanger. She has conducted research on societal security and protection of critical infrastructures since 1996. Since 2005, her work has been directed towards information security and societal security, the last years also covering information operations, strategic communication and the vulnerability of the digital society. Janne Hagen has been a member of several expert groups in Norway and also worked in EU funded projects. She was a member of the Norwegian Committee of Digital Vulnerabilities in Society. The Committee delivered an Official Norwegian Report (NOU) to the Ministry of Justice and Public Security in 2015.

This threat development was foreseen and well warned. Twelve years ago, the security expert Bruce Schneier predicted that fast automation attacks—hazardous actions at distance—and technique propagation would become a significant threat as it required only one skilled attacker; other attackers could simply copy and use their tools.<sup>[1]</sup> Since 2004, the conditions pointed out by Schneier have been further aggravated, helped by unpatched vulnerabilities and incorrect configurations. Today, the market for malware and exploits has matured, as documented by a RAND Corporation study.<sup>[2]</sup> State actors, organizations, and individuals participate and trade in this market. All that is required to purchase malware and cybercrime services are a web browser and a credit card. Many tools and services are furthermore available at affordable prices—some are even free of charge. The consequences are enormous, as pointed out by Rhoades and Twist (2015):<sup>[3]</sup> the high profile data breaches during 2015 include, among others, the Snapchat 4.5 million names and phone numbers, the eBay database of 145 million users compromised, the UCLA Health 4.5 million records, the Army National Guard 850,000 records and more.

Pell and Soghoian in 2014, examined the historical perspective of security challenges in the mobile networks, showing how the US government disregarded the security challenges. In 1993, American policy makers took no actions in order to force the industry to improve the exposed technical security flaws in the analogous telephone technology. Instead, they prohibited eavesdropping equipment that could be used to exploit the weaknesses.<sup>[4]</sup> This strategy did not pay off in the long run. When the mobile networks became digitized, they remained vulnerable, while the eavesdropping equipment was improved and became cheaper at the same time. Today, even



Dr. Olav Lysne is Director and founder of the Center for Resilient Networks and Applications (CRNA) at Simula Research Laboratory, and professor in computer science at Simula and the University of Oslo. He received the Master's degree in 1988 and the Doctor of Science in 1992, both at the University of Oslo. The early research contributions of Lysne were in the field of algebraic specification and term rewriting, with a particular emphasis on automated deduction. While working in this field he was a visiting researcher at Université de Paris-Sud. Later in his career he has been working on resilient computer architecture for supercomputing and cloud infrastructures, routing and switching techniques for IP-networks and measurement of national network infrastructures. Lysne was the leader of the Norwegian Government's Commission on digital vulnerability, which submitted its report to the Minister of Justice and Public Security in November 2015.

amateurs can gain wireless access to and use these tools and software to tap mobile phone calls.

Through the Internet, the world has become globally interconnected. All nation states are increasingly exposed to cyber threats and cyber-crime from abroad. In the cyber domain, there are no physical borders, and *traveling* around the world is now possible, digitally speaking, in a microsecond. The world—with both good and bad actors—has entered our homes and businesses through cyberspace. It is not surprising then, that security authorities, and the military sector are concerned and aim to develop policies, plans, tools and modes of operations to defend the homeland. In this global cyber world, however, good security inventions, like for instance surveillance software, can later on be stolen and used against law abiding citizens. This brings us back to the challenge of evaluating and balancing surveillance versus privacy. On one hand, surveillance tools are in great demand, but on the other hand, they could become dangerous in the hands of an adversary, for instance a criminal organization, or a state in a potential conflict. Balancing surveillance and privacy is therefore very intricate, and hence of great importance, as raised by the Official Norwegian Report (NOU) to the Minister of Justice and Public Security.<sup>[5][6]</sup>

The rest of this article is structured in the following way: In section 2, we introduce the Norwegian case of digitalization; the policy of modernization and digitalization, and a brief introduction to digital vulnerabilities. In section 3, we discuss the society's need for security and privacy to fight crime and terror. In section 4, we turn to the privacy issues and argue why privacy matters. Section 5 deals with the challenge of balancing surveillance and privacy, and section 6 presents the conclusion.



## 2. CASE: THE NORWEGIAN DIGITIZED SOCIETY

### *2.1 The Digital Agenda for Norway*

The Norwegian government's white paper on the Digital Agenda for Norway<sup>[7]</sup> presents the government's policy on how the Norwegian society should benefit from value creation and innovation opportunities offered by information technology and the Internet. The Digital Agenda adopts a long-term perspective, 2020.<sup>[8]</sup> According to the policy document, widespread online participation represents a comparative advantage to the country and provides a variety of benefits for the citizens. The high political ambitions for digital participation are summarized here:<sup>[9]</sup>

- ◆ Everyone in Norway who wishes to use digital tools and services should be able to do so.
- ◆ Provisions will be made to ensure relevant training opportunities for groups that need them.
- ◆ Within five years, the number of citizens not online will be halved, from 270,000 to 135,000 (Norway has about 5.2 million inhabitants).
- ◆ The education system will provide individuals with sufficient qualifications to continue developing their digital competence and keep pace with technology developments.
- ◆ Employees will be able to use digital tools and develop their digital skills at work.
- ◆ The population will have sufficient skills to use the Internet safely and securely.

Digitization has been driven by huge cost savings, new income opportunities, and future product innovations and business developments. According to Ark and Inklaar in 2005, as much as 50 percent of European productivity growth was attributed to the use of information and communication technology (ICT) and the Internet.<sup>[10]</sup>

Today, Norway is a highly digitized society. The majority of Norwegians have access to the Internet at home, 98 percent have mobile phones, and 80 percent have smart phones (2014).<sup>[11]</sup> Digitization has infiltrated all parts of modern society. Physical payment accounts for less than 5 percent of all transactions; the finance sector is digitized and it is difficult to get cash—even when visiting a bank. Smartphone applications now enable people to pay their bus and train tickets electronically from their mobile phones. Citizens also have access to their electronic patient journal from the Internet, and medical prescriptions can be provided electronically. The individual reporting to tax authorities is done electronically, with most of it by algorithms that automatically collect data from

a variety of registries. Internet voting has been on trial, and the preferred way for contact between the citizens and the authorities is through a web interface and Internet connection. Norwegian authorities aim furthermore to meet the population on social media, where the majority of the population is active. Within a few years, the electrical power grid rolls out smart digital meters, which enables the development of more digitized welfare and health services on the top of the meter infrastructure. These services will, among other things, help the elderly to stay longer in their homes. The country's welfare, income creation, and security depend increasingly on bits and bytes carried by the Internet Protocol (IP) wired or by air.

The digitization project has brought Norway to the top ranking in Europe and number four globally according to the Cyber Security Index<sup>[11]</sup> but digital vulnerabilities still remain. The complexity and the risk of failure are given by the long digitized value chains that stretch across national borders, by the traffic data and the signaling data that flows constantly. If you want to pay your bus ticket with the ticket app, the electronic money transfer depends on the functionality of every long chain of various service providers, Internet and telecom providers, satellite services like accurate time and various technical systems; a chain from the mobile app and your bank server, and all the way to the bank account of the bus company. Your mobile phone is always connected, and the signaling data leaves traces of the location of the device.

---

---

The intricate challenge  
is that in-between the  
surveillance and the privacy  
lays the personal data—  
the new gold...

## ***2.2 The threats towards the digitized society***

Cyber threats grew out of the huge digitalization project with the opportunities and vulnerabilities that followed. According to the Norwegian Computer Crime Survey 2014, most cyberattacks misuse old and known vulnerabilities that are not supported or patched. Although Norway is a wealthy country, and in the frontline of digital technology adaption, the old unpatched systems show up as an important vulnerability that enables an attacker to gain unauthorized access to information and systems.

The results from the Norwegian Computer Crime Survey in 2014 documents that more than half of Norwegian enterprises have been hacked, not just 5 percent as the respondents in the survey reported. This conclusion was derived by a comparison of data of the Computer Crime Survey with data from Mnemonic, a Norwegian security company, and NSM NorCERT. Table 1 shows the number of hacking incidents detected in large Norwegian companies reported by the survey or detected by Mnemonic and NSM NorCERT. The results show that the ability to detect incidents is limited; of the reported hacking incidents in the survey, only 1 percent is reported to the police.<sup>[13]</sup>



Table 1. Detected hacking incidents in large Norwegian companies, 2014.<sup>[14]</sup>

Hacking Incidents in Large Companies	The Norwegian Computer Crime Survey 2014	Mnemonic	The Norwegian National Security Authority (NSM NorCERT)
Number of Hacking Incidents Reported	600	444	51
Percentage of Enterprises Experiencing Hacking	5	66	50

### 2.3 The use of cloud computing and the Snowden revelations

The use of cloud computing is on rise in Norway with two-thirds of Norwegian enterprises reported using cloud computing services in 2014. According to the Norwegian Computer Crime Survey 2014, the use of cloud services may be a favorable solution for the many small enterprises in Norway that otherwise lack sufficient IT security knowledge and enough resources to build and run secured IT systems.<sup>[15]</sup> International cloud computing service providers represent increased technical security (better patching regime and remote backup), but at the same time, the use of cloud computing means reduced national control. The challenges with surveillance versus privacy exploded in 2013, when Edward Snowden, who worked for a contractor, Booz Allen Hamilton, leaked numerous classified documents about National Security Agency (NSA) intelligence programs.<sup>[16]</sup> The Snowden leakages of the massive NSA surveillance program struck directly at privacy issues and the Safe Harbor regulation. The Safe Harbor regulation allowed companies operating in the European Union (EU) to send personal data to third countries outside the European Economic Area. In October 2015, the European Court of Justice responded to a referral from the High Court of Ireland concerning a complaint from an Austrian citizen, Maximillian Schrems, regarding transfer of his Facebook data to the US in the aftermath of the Snowden revelations. The European Court of Justice then held the Safe Harbor Principles to be invalid.<sup>[17]</sup> The Maximillian case illustrates the paradox between surveillance and privacy, and how it can hit back on commercial interests and trust.

There are two observations that can be made so far regarding the cyber environment. First, we are entering into a future where close to everything we do, will have a digital component. Most of our activities will be communicated over a network and can potentially leave a digital trace. This means that close surveillance of every individual in a society is becoming technically feasible, and thus constitutes a serious threat to privacy as a human right. The second observation is that criminal activity, ranging from amateur hacking to terrorist attacks, will also have a digital component. The same mass surveillance that is a threat to our human rights is also a powerful, and sometimes a necessary tool to ensure our security. We elaborate further regarding this dilemma in the upcoming sections.

### 3. THE SOCIETY'S NEED FOR SECURITY AND SAFETY

#### ***3.1 Incident detection and handling***

As society becomes more digitized, vulnerable and complex, the need for continuous monitoring and surveillance of critical systems, security warnings, and incident handling services increase. Surveillance can have beneficial political impacts where it detects fraud.<sup>[18]</sup> A system that monitors the banking industry and money transfers might support democracy by making corporate wrong-doing harder to hide.

The number of Computer Security Incident Response Teams (CSIRT) and Computer Emergency Response Teams (CERTs) in Norway is growing. Many of these institutions provide incident monitoring, warning, and incident handling services that will aid enterprises to detect and be aware of the attacks.

NSM NorCERT is the national CERT, which is coordinating incident handling in critical infrastructures and important societal services, in addition to operating a national warning system for critical infrastructures. There is a close cooperation between the intelligence services, the security police, and NSM NorCERT.<sup>[19]</sup>

In addition to this national CERT, there are several sector or industry based CERTs and CSIRTs. The Norwegian defense sector's CSIRT serves the military forces. In civil society, the CERT of the national universities, UNINETT CERT, manages computer security incidents that target, originate from or misuse the networks or connected equipment belonging to UNINETT or its member institutions.<sup>[20]</sup> Health CSIRT is the joint information security competence center for the Norwegian health care sector. The center shares knowledge about ICT threats and protection mechanisms, and continuously monitors traffic within the health network. The goal is to prevent and remediate adverse ICT security incidents and malicious intrusion attempts.<sup>[21]</sup> FinansCERT is dedicated for the Norwegian financial

---

---

The digitization project has brought Norway to the top ranking in Europe and number four globally according to the Cyber Security Index ranking.

sector, as represented by Finance Norway (FNO). FinansCERT serves banks, life insurance and pension companies that are members of Finance Norway.<sup>[22]</sup> The Norwegian KraftCERT was established in October 2014. KraftCERT provides information sharing between companies and organizations both nationally and internationally and assist the energy sector in handling digital security incidents. KraftCERT participates in the national emergency response organization.<sup>[23]</sup> In 2015, a CSIRT was established in the telecom sector, and a Municipality CSIRT is currently discussed.<sup>[24]</sup> In addition to these CSIRTs and CERTs, private companies offer monitoring and incident handling services.

The evolvement of the various CERTs and CSIRTs in Norway illustrates an important national effort for the monitoring of digital systems. This priority is driven by recognizing it is impossible to prevent all hacking incidents that Norwegian enterprises are exposed to, and that authorities and businesses should prepare to detect and handle the incidents when they occur.

### ***3.2 Police internet patrolling and covert operations***

Digitization itself has enabled more efficient systems, network surveillance, and more effective data analytics. By combining different sources of digitized data and using statistics and algorithms, new insight can be produced, giving better situational awareness, improved decisions, and more efficient operations.

Since criminal activities also have become digitized, law enforcement must visibly patrol the Internet. In addition, the police may need to operate covertly. To investigate serious crime and predict crime or terror attacks, predictive analysis, access to social media accounts and big data analytics could provide significant aid for law enforcement. With the latest Paris terror attacks in November 2015, it is not difficult to understand the importance of eavesdropping and the need to intercept mobile phone calls of suspects as described by Pell and Soghoian.<sup>[25]</sup>

Signaling information is generated even when the phones are not used. The signaling data provides information about geo-localization, hence personal information. Law enforcement request three types of requests for information from telecommunication enterprises:<sup>[26]</sup>

- ◆ Requests for subscription data that can be given.
- ◆ Requests for traffic and signaling data, where the Norwegian Communication Authority can by law accept the request and release the internet and telecom provider's non-disclosure commitment. It has been argued that release of traffic data is less interfering for privacy than release of signaling data. Traffic data are generated by an action by the mobile phone user, in contrast to signaling, where data are transferred all the time irrespective of any positive action from the mobile phone user and reveals the geographical position of the user.
- ◆ Requests for communication control, for instance interception of mobile phones that requires a court order.

The Committee on Digital Vulnerabilities recommended a strengthening of the police's ability to combat cybercrime by establishing a new Cyber Crime Center. The Committee observed that among businesses and individuals there are low expectations as regards the assistance provided by the police to the victims of cybercrime.<sup>[27]</sup> This means that only a small percentage of cybercrime is reported, also documented by the Norwegian Computer

Crime Survey 2014. Therefore, the Committee supports the proposal to establish a new national center to prevent and investigate complex and cross-sectoral cybercrime. The center should be organized under the National Criminal Investigation Service (NCIS, Kripos), and it should have a national technical responsibility for the prevention and investigation of serious and complex cybercrime. It should also have a separate assistance function to support the 12 police districts both with respect to police tactics and prosecution.<sup>[28]</sup>

#### 4. CHALLENGES FOR HUMAN RIGHTS IN THE CYBER DOMAIN

The concept of human rights developed as a result of the World War II (WWII) and the Nazi regime's crime against humanity, and was further influenced by later conflicts and human rights violations. According to the Universal Declaration of Human Rights (UN, 1948), every individual has the right to life, liberty and security of person, and the right to privacy. Article 12 states for instance: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."<sup>[29]</sup>

Everyone has the right to protection under the law against such interference or attacks. Does the IT industry and the political decision makers take into account how human rights could be affected when they design and develop our digitized society? One example can illustrate the challenge: A misconfigured database leaking the personal information of over 191 million American voters was reported to DataBreaches.net by researcher Chris Vickery in December 2015.<sup>[30]</sup> According to DataBreaches.net there were no social security numbers, driver's license numbers, or any financial information in this particular database—but it contained information about the voters' full name, date of birth, address and phone number, together with political party and other fields. A police officer expressed his concerns as it became apparent that criminals now could find his home address.<sup>[31]</sup> In the long run, however, this kind of information can be used to obtain access to more private information about individuals. Even if it does not matter much today, it is just a question of time before it is possible to profile individuals, and then use this information to steal and misuse this person's digital identity, and to blackmail or threaten.

In fact, the vast amount of information stored on unsecured servers and in registries represents huge challenges for privacy and human rights. This challenge is illustrated with the current European refugee crisis: Norway, like other European countries, has in 2015 experienced a flow of refugees seeking a safe life in Europe. The refugees have escaped regimes that do not respect human rights, deny freedom of speech, and discriminate religion and political opinion. If the IT industry and government build data registries and IT systems that do not protect personal information, this might work well enough as long as the society remains safe, democratic and politically stable. In a potential future situation with a regime shift, new challenges and security issues might arise. For those who fled from the dangers in Syria and other countries, secure data registries containing personal information are a requirement to start a safe new life.

But there is another future security challenge. When society gets fully digitized, where can persecuted people, with digital identities shaped over time, escape? Is it possible to start a new life, to get a new digital identity? Is this possible if your digital biometric templates are stolen and disseminated?

A Swedish TV2 documentary, *You've Been Googled*,<sup>[32]</sup> highlighted this issue. According to the documentary, digitized and searchable information did not fully disappear, and old traces of information, wrong or correct, remained on the Internet, accessible by search engines. In one case an identity theft, in which the innocent victim's identity was mis-used for criminal purposes, stopped the victim's future job career. The big question is: Will there be any opportunities for a new start? In May 2014, the European Court of Justice (ECJ) ruled that internet search engines must remove information deemed "inaccurate, inadequate, irrelevant or excessive" for the purposes of data processing, or face a fine.<sup>[33]</sup> Will it be possible to enforce this regime, or have the policy makers made a similar mistake as they did in 1993 with cellular surveillance equipment?<sup>[34]</sup> So far, even if removal requests are granted, those same articles are still available online

at the sites where they were originally published or at google.com where the US version of Google is hosted.

---

Close surveillance of every individual in society is becoming technically feasible, and thus constitutes a serious threat to privacy as a human right.

On one hand, social media and the Internet support human rights by providing a platform for free speech and information sharing, but on the other hand, the use of the same technology

might restrain for instance free speech and thus cause a chilling effect.<sup>[35]</sup> What will be the long term impact of hate speech and harassment on the Internet? Will political discussions gradually diminish? It is well known that in several parts of the world, free speech is a risky business and bloggers 'just' disappear. So far, inhabitants of western democratic countries have the opportunity to speak out, but will this freedom last if everything we do and express are searchable on the Internet? According to Wright and Raab,<sup>[36]</sup> surveillance technologies can have harmful psychological impact on individuals' sense of privacy. If people know that they are being surveilled, they are likely to be more cautious than they might otherwise be. This is the *chilling effect* seen from the standpoint of its psychological effect, not to mention its social consequence.

## 5. BALANCING PRIVACY AND SURVEILLANCE

Until recently, there have been strict legal, economical, technological and practical limits to how surveillance could be used. If someone wanted to wiretap a phone call, they

connected an extra wire to a physical phone line. The phone call needed to be recorded on tape, and the tape required a human listener in order to be interpreted. Furthermore, the fraction of human activity leaving a trace on a phone line was limited. Therefore, the regulation of surveillance only needed to address a very limited number of cases. As mass surveillance of almost all activity of every citizen is becoming technically and economically feasible, the balance between surveillance and privacy is no longer given to us through the limits of what is doable. Wright and Raab<sup>[37]</sup> assess the political impacts of a surveillance system by asking a few questions: Who is being surveilled by whom and for what purpose? Who has authorized the surveillance? Will the project or technology enhance the power of some at the expense of others? Who will have access to the data gathered by a surveillance system and how will such data be used? Will it undermine the electorate's trust in their elected officials? Will the surveillance system support or undermine democracy?

Technical monitoring raises questions about surveillance and privacy. One such dilemma was raised in an article by Sveinbjørnsson in 2012.<sup>[38]</sup> In order to protect informants, the Norwegian national broadcasting company NRK decided to exit the monitoring and sensor services provided by NSM NorCERT. NSM NorCERT's response to this decision was that the sensors could be regarded as a kind of intrusion alarms, and if they were removed, intrusions would not be detected. Thus, any successful undetected hacking could disclose the informants' personal information anyway. The NRK later decided to join the NSM NorCERT's monitoring and sensing services.<sup>[39]</sup>

Also, covert operations conducted by law enforcement raises important questions about the value and balance between human rights, the right to free speech, privacy, and the rule of law. The Norwegian official report (NOU 2015:13) points to the challenges of using signaling data from telecommunication providers for other purposes than originally applied for. This challenge should be studied in more detail. Law enforcements extensive use of signaling data indicates it might be necessary to regulate the access to such data.<sup>[40]</sup>

Almost everywhere, you can travel virtually along the public roads by using Google Street View. People and vehicle identities are anonymized, but you can zoom to a high degree and study the houses and gardens. Norwegians have a high level of trust in government, enterprises and their fellow citizens. In Germany, in contrast to Norway, Google Street View is not offered. The reason is Germany's WWII history and the raised awareness of the value of privacy after the Snowden leakages. In Germany, 70 percent of the population do not accept that the government surveils data traffic and phones.<sup>[41]</sup> It is now 75 years since WWII and the occupation of Norway. In retrospect, if Norway was digitized during WWII, what digitized information would be accessible for the occupants about the enlisted youth in the military and about those who sympathized with the opponents of the Nazi regime? What intelligence advantages could be gained about the enlisted in the army by the use of predictive analysis based on social media utterings? How could meanings and



utterings by opponents be analyzed and interpreted as coming actions?

When the Islamic extremists went underground and used encryption, the need for new intelligence methods arose. According to the Norwegian newspaper Aftenposten, the Norwegian Police Security Service wanted to install key loggers on suspects' devices.<sup>[42]</sup> It is a well understood demand from a counter terrorism perspective, but it raises some challenges from a privacy and human rights perspective: One is the potential strength of electronic data in court compared with for instance voice tapping, another is the risk for surveilling innocent persons. A third challenge is to ensure that the intent of the written text is correctly understood.

A comment in Journal of Criminal Law, Criminology and Police Science (1970) states that "The courts should not be willing to permit the state to employ techniques of stealth and deception to obtain information which it is prohibited from obtaining by means of unrestricted wiretapping, legislative inquiry, or search and seizure. The state's license to secretly survey and eavesdrop should be subject to more than only the unfettered discretion of police officials".<sup>[43]</sup> Today, this challenge has moved into the cyber domain. In the NOU 2015:13 the governmental committee notes that the interests of public safety lead to proposals to introduce new and intrusive surveillance methods.<sup>[44][44]</sup> Examples are proposals to introduce digital border surveillance and the Norwegian Police Security Service's desire to register utterances on social media, and to analyze information from open channels. The committee further acknowledges the police and intelligence agencies' needs behind such proposals, but argue that the proposals are of such an intrusive nature that they should not be introduced without prior public debate. Such a debate should be prepared through a public report that discusses these types of measures in full. Intelligence needs, technological expertise and protection of privacy must be safeguarded, and a thorough report must be made on the technological, legal and social issues the cases raise.

---



---

If people know that  
they are being surveilled,  
they are likely to be more  
cautious. This is the chilling  
effect seen from the stand-  
point of its psychological  
effect, not to mention its  
social consequence.

The committee has also pointed to the international debate on whether the use of strong cryptography should be regulated. It is extremely difficult—perhaps impossible—to develop systems that safeguard legitimate needs for protection and monitoring at the same time. It is therefore reasonable to believe that any limitations in the lawful use of cryptography will

affect Norwegian citizens, businesses and authorities. Any limitations on cryptography will at the same time not deter dishonest players from using cryptography and therefore not solve the police and the intelligence services' problem either. That is why the committee believes that use of cryptography should not be regulated or banned in Norway, moreover the Norwegian authorities should work actively against regulation or prohibition internationally, and that new investigation methods must be developed to ensure efficient law enforcement and intelligence work.<sup>[45]</sup>

## 6. CONCLUSION

Digitization has opened up borders and made it possible to exchange ideas and thoughts worldwide. It has enabled new business concepts and increased information flow and effectiveness. Many voices not previously heard can now get attention through social media and blogs. An increase in global cybercrime, mass surveillance, Internet censoring and espionage has however followed this technological development, and with this development a subsequent need for surveillance of crime and terror investigation. In retrospect, the mobile phone surveillance case in 1993 illustrated the risk that adversaries will utilize the technological opportunities and developed tools. The 1993 case also demonstrated that legal measures alone are not enough when the technological development provides cheap opportunities for surveillance and eavesdropping for anyone.

It is well documented that digital systems are vulnerable to espionage as well as physical and electronic sabotage. It is reasonable to believe that the complexity and lack of transparency of the digital value chains together with old versions and unpatched systems will remain a security headache in the future. An even bigger nightmare might be loss of privacy and misuse of personal information. With access to data registries and the ability to merge and analyze personal information, including personal utterances and movements over time, an adversary can steal identities, blackmail and pose huge pressure towards single individuals and groups of people. At the very end it will become easier to select single individuals, key players in society as well as children. From a counter terrorism perspective increased surveillance would be a good idea, but the flip side of the coin would be that the surveillance capacity could be used against citizens sometime in the future. This could next threaten the population's trust in government, national security, and societal stability.

The intricate challenge is that in-between the surveillance and the privacy lays the personal data—the new *gold* from a commercial perspective, a resource in the fight against terrorism from a security perspective, and a future threat of human rights from an individual perspective. There is no simple solution to the paradox. The Norwegian report (NOU 2015:13) recommends not regulating encryption, and that any eavesdropping and surveillance for the purpose of fighting crime or enhancing national security should have a foundation in national law and sanctioned through public debate. Finally, an



enormous responsibility is laid on industry to design products and software that protect privacy, i.e., privacy by design.🛡️

## ACKNOWLEDGEMENTS

We would like to thank Ms. Eva Jarbekk, Lawyer and partner of Føyen Torkildsen Advokatfirma AS and member of the Norwegian committee of privacy (Personvernneemda) for contributions to the article. We would furthermore thank Mr. Bjørn Olav Knutsen (Principal Scientist at FFI and Associate Professor at the University of Nordland), Mr. Torgeir Broen and Torkjel Søndrål, Senior Scientists at FFI, the Research Managers Ms. Hilde Hafnor and Mr. Ronny Windvik at FFI for comments, and finally, Ms. Ålov Runde Language Advisor at FFI, for spell check and language vetting.

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

## NOTES

1. Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World, with New Information about Post-9/11 Security*, 2nd ed., (Indianapolis: Wiley Publishing, 2004), 14-22.
2. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime. Tools and Stolen Data. Hackers' Bazaar* (Santa Monica: RAND Corporation, 2014) [http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR600/RR610/RAND\\_RR610.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf) (accessed December 29, 2015).
3. Blake Rhoades and Jim Twist, "Our Data is Not Secure", *The Cyber Defense Review Blog*, published October 2015 <http://www.cyberdefensereview.org/2015/10/28/our-data-is-not-secure/> (accessed January 5, 2016).
4. Stephanie K. Pell and Christopher Soghoian, "Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy", (*Harvard Journal of Law and Technology*, 28 Number 1 Fall, 2014), 1-35. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2437678](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678) (accessed December 29, 2015).
5. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden*. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
6. Committee of Digital Vulnerabilities in Society – Summary, Official Norwegian Report (NOU 2015: 13) to the Ministry of Justice and Public Security 30. November 2015 <https://www.regjeringen.no/contentassets/fe88e9ea8a354bdlb63bc0022469f644/no/sved/9.pdf> (accessed January 5, 2015).
7. *Digital Agenda for Norway — Meld. St. 23 (2012–2013) Report to the Storting (white paper)*, <https://www.regjeringen.no/en/dokumenter/meld.-st.-23-2012-2013/id718084/?ch=1&q=> (accessed December 29, 2015).
8. Ibid., chapter 1.
9. Ibid., chapter 2.
10. Bart van Ark and Robert Inklaar, *Catching up or Getting Stuck? Europe's Troubles to Exploit ICT's Productivity Potential*, Groningen Growth and Development Centre, Research Memorandum GD-79 (University of Groningen, 2005) <http://www.rug.nl/research/portal/files/2856698/gd79online.pdf> (accessed December 29, 2015).
11. Statistikkbanken, SSB, Statistics Norway, <https://www.ssb.no/statistikkbanken/SelectVarVal/saveselections.asp> (accessed January 7, 2015).
12. *Global Cyber Security Index*, (New York: ABI Research, 2014) <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf> (accessed December 30, 2015).
13. Mørketallsundersøkelsen, Informasjonssikkerhet, personvern og datakriminalitet 2014 (the Norwegian Computer Crime Survey), Næringslivets sikkerhetsråd (NSR), [http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall\\_2014\\_WEB.pdf](http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014_WEB.pdf) (accessed January 8, 2015).
14. Ibid.
15. Ibid.
16. Laura Poitras and Glenn Greenwald, *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'* – video, (Hong Kong: The Guardian, 2013) <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video> (accessed January 8, 2015).
17. "International Safe Harbor Privacy Principles", article, Wikipedia, [https://en.wikipedia.org/wiki/International\\_Safe\\_Harbor\\_Privacy\\_Principles](https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles) (accessed January 8, 2015).
18. David A. Wright and Charles D. Raab, "Constructing a surveillance impact assessment", (*Computer law & security review* 28, 2012), 619.
19. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden*. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014. Avgitt til Justis- og beredskapsdepartementet November 30, 2015. (In Norwegian)
20. UNINETT CERT – Policy and service level statement, published 6th June 2015, <https://www.uninett.no/cert/policy.html> (accessed January 7, 2015).
21. Health CSIRT, Helsenet, home page <https://www.nhn.no/english/Pages/HealthCSIRT.aspx> (accessed January 5, 2015).
22. FinansCERT, Norwegian Financial CyberCrime Unit, home page, <http://www.finanscert.no/engelsk.html> (accessed January 5, 2015).

## NOTES

23. KraftCERT, home page <https://www.kraftcert.no/english/index.html> (accessed January 5, 2015).
24. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
25. Stephanie K. Pell and Christopher Soghoian, “Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy”, (*Harvard Journal of Law and Technology*, 28 Number 1 Fall, 2014), 1-35, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2437678](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678) (accessed December 29, 2015).
26. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet November 30, 2015. (In Norwegian)
27. Ibid.
28. Ibid.
29. Universal Declaration of Human Rights, United Nations, 1948, <http://www.un.org/en/universal-declaration-human-rights/index.html> (accessed December 30, 2015).
30. 191 million voters’ personal info exposed by misconfigured database (UPDATE2), Databreaches.net, published December 28, 2015 <http://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/> (accessed January 8, 2015).
31. Ibid.
32. “Du är Googlad” (You are googled), Documentary (in Swedish), Swedish TV, with Nikke Lindqvist, Brit Stakston, Johan Ripås, Tina Ax och Bengt Gangemi. (Published April 11, 2012) <https://www.youtube.com/watch?v=6JFlvZV2VM> (accessed March 5, 2015).
33. Curtis, Sophie, “EU ‘right to be forgotten’: one year on”, published May 13, 2015 <http://www.telegraph.co.uk/technology/google/11599909/EU-right-to-be-forgotten-one-year-on.html> (accessed December 30, 2015).
34. Stephanie K. Pell and Christopher Soghoian, “Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy”, (*Harvard Journal of Law and Technology*, 28, Number 1 Fall, 2014), 1-35 [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2437678](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678) (accessed December 29, 2015).
35. David A. Wright and Charles D. Raab, “Constructing a surveillance impact assessment” (*Computer law & security review* 28, 2012), 619.
36. Ibid.
37. Ibid.
38. Sveinbjørnsson, Sigvald, “NRK kastet ut statens «spionboks», (Publisert November 5, 2012) <http://www.digi.no/sikkerhet/2012/11/05/nrk-kastet-ut-statens-spionboks> (accessed December 29, 2015).
39. Kabakk, Per Arne, “Elektronisk kildevern i NRK”, comment, NRK, published 19th September 2014 <http://www.nrk.no/ytring/elektronisk-kildevern-i-nrk-1.11941196> (accessed January 7, 2015).
40. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
41. Jørgensen, Sten Inge, *Tyskland stiger frem*, Oslo: Aschehoug, 2014.
42. Olav Døvik, Camilla Wernesén, and Mon, Su Tiet, “PST vil overvåke datatastaturer”, NRK, published 04. March 2014 <http://www.nrk.no/norge/pst-vil-overvake-datatastaturer-1.11583286> (accessed January, 5, 2015).
43. Police Infiltration and dissident groups, comment (*The Journal of Criminal Law and Police Science* 61 2, 1970), 194.
44. NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker i en digitalisert verden. Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014*. Avgitt til Justis- og beredskapsdepartementet 30. november 2015. (In Norwegian)
45. Ibid.

# Cyber Risk Assessment in Distributed Information Systems

---

Dr. Kamal Jabbour

Major Jenny Poisson

## ABSTRACT

**T**his paper presents a disciplined approach to cyber risk assessment in distributed information systems. It emphasizes cyber vulnerability assessment in the architecture, specification and implementation—the knowledge of us—as a vital first step in estimating the consequence of information compromise in critical national security systems. A systematic methodology that combines information flow analysis and Byzantine failure analysis allows assessing the effects of information integrity compromises and the development of a Blue Book to guide cooperative Blue Team testing. The analysis of system vulnerability extends to cyber threats—the knowledge of them—leading to the development of a Red Book to inform adversarial Red Team testing. The paper concludes with a notional case study that illustrates this approach.

## 1. INTRODUCTION

### *1.1 Risk*

In 2002, the National Institute of Standards and Technology (NIST) defined risk to information systems as “a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event” and a threat as “the potential for a particular threat-source to successfully exercise a particular vulnerability.”<sup>[1]</sup> Although the 2012 Guide for Conducting Risk Assessments<sup>[2]</sup> that superseded the 2002 document redefined risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence,” we like the simplicity of breaking risk into three fundamental components: vulnerability, threat and impact.

In complex distributed information systems, such as an aircraft, satellite or an air



Dr. Kamal T. Jabbour, a member of the scientific and technical cadre of senior executives, is Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, in Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry. Dr. Jabbour is an avid distance runner who has run marathons in all 50 states.

operations center, Cyber Vulnerability Assessment (CVA) focuses on identifying architectural features, specification requirements, and implementation artifacts that form an attack surface that a threat adequately resourced in time, talent and treasure can exploit. While a thorough CVA requires an understanding of threat capabilities, a CVA remains essentially an exercise in the knowledge of us.

NIST characterizes a threat source as “the intent and method targeted at the exploitation of a vulnerability.” In our cyber risk assessments, we assume intent and we focus on understanding and quantifying the threat capability necessary to exploit a known vulnerability. As such, threat and vulnerability go hand in hand—there is no threat where there is no vulnerability. Granted, we must treat both threat and vulnerability as probabilities, rather than binary zeroes or ones. We analyze a system for vulnerabilities, and we estimate the probability of a threat exploiting each vulnerability, where characterizing the threat requires understanding adversary capability in terms of time, talent and treasure—the knowledge of them, as well as access means—remote, physical and supply chain.

A successful threat exploitation of an information system vulnerability provides the mission owner or commander the third component in the risk calculus, impact, and permits risk management decisions. The risk calculus consists of a vulnerability—which the mission commander owns—a threat capability necessary to exploit the vulnerability—which the adversary owns—and the impact of a successful threat exploitation of the vulnerability—which we measure in terms of disruption, degradation, denial, destruction or deception. In this paper, we use interchangeably the terms impact, effect and consequence based on the context.



Major Jenny M. Poisson is an Executive Staff Officer for the Secretary of the Air Force (SecAF) and Program Manager for SecAF Advisory Board Studies, Air Force Scientific Advisory Board, Pentagon, Washington, D.C. She is responsible for conducting studies on topics deemed critical to the Air Force mission and recommends applications of technologies that can improve Air Force capabilities. Major Poisson also serves as Individual Mobilization Augmentee (IMA), to the Air Force Senior Scientist for Information Assurance, Air Force Research Laboratory Information Directorate, in Rome, NY. In this role, she assists and advises the Senior Scientist in conceiving, planning and advocating for major research and development activities. Major Poisson leads a Total Force Blue team to act as trusted agents and honest brokers to the USAF on cyber vulnerability assessment of weapons and missions. In the process, the team identifies areas for Science & Technology insertion in both the test process and vulnerability mitigation, and informs the development of future systems.

### ***1.2 Information Assurance***

Joint Publication 1-02, Department of Defense (DoD) Dictionary of Military and Associated Terms,<sup>[3]</sup> defines information assurance (IA) as the “actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality and nonrepudiation.” We differentiate between the actions that apply to information—confidentiality, integrity and availability—and those that deal with users and processes—authentication and nonrepudiation.

Information assurance professionals recognize the first three goals of confidentiality, integrity and availability as the tenets of information assurance. In assessing the cyber risks to distributed information systems, we examine the impact of compromises in the confidentiality, integrity and timely availability of information critical to a mission, regardless of the means by which such compromises occur. This approach permits us to separate vulnerability and impact—the *what*—from threat—the *how*.

### ***1.3 Mission Assurance***

DoD Directive 3020.40 defines Mission Assurance (MA) as “a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy.”<sup>[4]</sup>

In accordance with this directive, the primary responsibility of a commander is to ensure the timely execution of his mission, while assuming a risk commensurate with mission vulnerabilities and the impact of a successful exploitation by a capable threat.

According to Air Force Doctrine Document 3-12 on Cyberspace Operations, “mission assurance entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.”<sup>[5]</sup>

Design specification documents provide a list of MEFs that constitute a mission. Prioritizing these MEFs rests with the mission owner, and depends on the operational environment for the mission, steady-state versus contingency, peacetime versus war, or escalation versus restoration.

Mapping mission dependence on cyberspace requires a detailed understanding of the mission. DoD Architectural Framework (DoDAF) Operational Views (OV) and Systems Views (SV)<sup>[6]</sup> provide good starting points for mapping mission dependence on cyberspace. A fractal approach to mission mapping permits increasing the fidelity and resolution of mapping a priority MEF at the expense of lower priority MEF with lesser mission impact.

Identifying cyber vulnerabilities requires an intimate knowledge of the architecture, specification and implementation of the priority MEF. First, architecture vulnerabilities

Information assurance professionals recognize the first three goals of confidentiality, integrity and availability as the tenets of information assurance.

result often from the overlap among safety, reliability and security requirements. While reliability requires *at least* this much functionality, security demands *at most* this much functionality, with the potential for excess functionality turning into vulnerability. Second, specification vulnerabilities resulting from policy mandates and protocol choices may increase the risk to an MEF. Third, implementation vulnerabilities, including hardware, software and configuration, open the aperture of vulnerability assessment to supply-chain and user considerations.

The final tenet of mission assurance, vulnerability mitigation, follows a three-pronged approach. First, Tactics, Techniques and Procedures (TTP) may suffice to mitigate certain implementation vulnerabilities. However, materiel solutions are often necessary to mitigate architecture and specification vulnerabilities. Where TTP fall short and materiel solutions do not exist, pursuing advanced Science and Technology (S&T) becomes necessary to create adequate mitigations that reduce the vulnerability and the likelihood of threat exploitation, increase the cost of a successful exploitation and reduce its adverse impact on the mission.

#### **1.4 Testing**

Cradle to grave mission assurance requires conducting outcomes-based Test and Eval-



uation (T&E) in a realistic threat environment, early and often in the acquisition lifecycle. T&E must include cyber threats that represent current and projected adversary capabilities. Developmental Test and Evaluation (DT&E) during pre-systems acquisition and Operational Test and Evaluation (OT&E) during acquisition and sustainment play vital roles in mission assurance. The earlier a test discovers cyber vulnerability, the lower is the cost of mitigating such vulnerability.

DoD Directives 5000.01<sup>[7]</sup> and 5000.02<sup>[8]</sup> provide the principles and policies governing T&E and identify the flow of T&E activities within the acquisition lifecycle. According to Defense Acquisition University, DT&E seeks to identify technical capabilities and limitations, stresses the system to ensure robust design, and assesses performance under a number of environmental parameters such as adverse weather, while OT&E seeks to evaluate the operational effectiveness and suitability of a system operating under realistic combat conditions.<sup>[9]</sup>

Cyber testing leverages the first three steps of mission assurance: prioritizing MEF, mapping MEF dependence on cyber, and identifying architecture/specification/implementation vulnerabilities. Both DT&E and OT&E must take the cyber environment into consideration as both an environmental parameter and as a hostile combat condition. While DT&E may limit its focus to the cyber vulnerabilities in a system and the potential impact of their exploitation, OT&E must examine the capabilities necessary to exploit these vulnerabilities in a manner that creates an adverse impact to the mission of the system.

It is imperative that cyber testing remain outcomes-based, and focus on the impact of a successful threat exploitation of a vulnerability in the architecture, specification or implementation of a mission, rather than compliance-based with a checklist of IA controls. We differentiate between cyber testing—testing a mission or system in a realistic cyber threat environment—from cybersecurity testing—testing for compliance with an arbitrary list of IA controls that are neither necessary nor sufficient for mission assurance.

### ***1.5 Paper Overview***

In the following sections, we present a systematic top-down approach to identifying potential cyber vulnerabilities in a complex information system through a disciplined information flow analysis, and estimating the mission impacts of information compromise. We apply Byzantine failure analysis to separate the impact of an information compromise

---

---

Identifying cyber vulnerabilities requires an intimate knowledge of the architecture, specification and implementation of the priority MEF.



from the underlying cause of the compromise, whether accidental or malicious. We advocate generating a Blue Book of cyber vulnerabilities at the end of this vulnerability assessment phase to guide the cooperative test activities by a Blue Team.

While a Blue Book of cyber vulnerabilities provides an introspective look at the engineering of the system under test, the subsequent development of a Red Book seeks to quantify the adversary capabilities necessary to exploit the cyber vulnerabilities that the Blue Book identifies. The Red Book provides Red Teams with a roadmap to conduct adversarial testing by a Red Team, and defines the threat capabilities that an aggressor team seeks to understand, replicate and exercise.

We complete our discussion of mission assurance by addressing vulnerability mitigation. We explore first Tactics, Techniques and Procedures (TTP) where applicable, then discuss materiel solutions when TTP fall short. Ultimately, mitigation may require pursuing Science and Technology (S&T) solutions. We conclude the paper with a simplified notional case study to illustrate our cyber testing approach.

## 2. CYBER VULNERABILITY ASSESSMENT

The 2011 paper on the Science of Mission Assurance<sup>[8]</sup> introduced the information lifecycle as a construct for representing information evolution in a complex system. It defined the six phases of information:

- ◆ Information generation,
- ◆ Information processing,
- ◆ Information communication,
- ◆ Information storage,
- ◆ Information consumption, and
- ◆ Information destruction.

The paper reasoned about a dozen hypotheses that govern mission assurance in the context of the information lifecycle, and we reached some obvious conclusions, including the fact that a closed system that does not exchange information with the outside world is not vulnerable to external information compromise.

The corollary to this conclusion is that a system that exchanges information with the outside world may be vulnerable to compromises in the confidentiality, integrity and availability of external information. This corollary constitutes the basis for our cooperative CVA.

### ***2.1 Information Exchange Boundary***

Defining the Information Exchange Boundary (IEB) constitutes the first step in a cooperative CVA. We interchange the use of the terms Mission under Test (MUT) or System under

Test (SUT), depending on the context, to refer to the distributed information assessment under study. The specificity of the IEB definition depends in part on the form factor of the SUT. It is easier to visualize the IEB for an orbiting satellite than it is for a space operations center with numerous networked radars and ground stations, industrial control systems and power supplies.

## ***2.2 Information Exchange Requirements***

System specification design documents define the Information Exchange Requirements (IER) for a platform or a system, and provide a good starting point for an exhaustive enumeration of the information exchanges between a SUT and the outside world through the IEB.

An essential step in a CVA is to characterize in details every information exchange in terms of:

- ◆ Protocol: for example Link-16, Voice over Internet Protocol (VoIP)
- ◆ Protocol layers in use: transport layer, application layer
- ◆ Medium: wired, wireless, optical, infrared
- ◆ Modulation scheme: analog or digital, Phase Shift Keying (PSK) or Quadrature Amplitude Modulation (QAM)
- ◆ Frequency or band: 2.4 GHz, S-band
- ◆ Data rate
- ◆ Encryption scheme
- ◆ Authentication mode
- ◆ Data compression scheme
- ◆ Header and payload formats
- ◆ Other relevant characteristics

## ***2.3 Adverse Cyber Effects***

Estimating the impact of an information compromise presents a significant challenge in cyber risk assessment. We seek to estimate the impact of an information compromise in terms of the D5 effects: disruption, degradation, denial, destruction or deception. We display these effects on a two-dimensional chart along the axes of degree and duration, as show in Figure 1.<sup>[11]</sup>

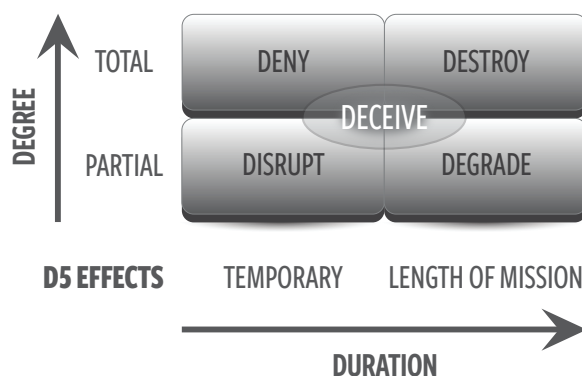


Figure 1. Effects in Relation to Degree and Duration

A thorough assessment of the impact of an information compromise necessitates decomposing the MUT into Mission Essential Functions (MEF), and estimating the effect on each MEF of a compromise in the confidentiality, integrity and availability of information flowing across the IEB.

Of the three IA tenets of confidentiality, integrity and availability, we focus first and foremost on the impact of compromises in information integrity. However, a compromise in confidentiality—someone else reading your good data—can also result in adverse mission impact. By the same token, reliability and safety requirements dictate redundancy in advanced information systems, permitting graceful degradation in the absence of certain critical information. In such a case, the absence of information, or a compromise in the availability of information, may be mitigated through redundancy.

The fifth D-effect, deception, can achieve any of the other four D effects by convincing a user or system of the presence or absence of an effect. We treat deception on par with the D4 effects of disruption, degradation, denial and destruction. While redundancy may mitigate a compromise in information availability, redundancy falls short in mitigating deception due to information integrity compromise. In a later section on S&T for mitigation, we explore trade-offs between information availability and information integrity, and seek to provide the mission owner a decision point: would you choose a radar that is available 100 percent of the time with a random 10 percent of the displayed information inaccurate, or one that is available 90 percent of the time with all the displayed information accurate?

## 2.4 Byzantine Failures

A reliable computer system deals with the failure of one or more of its components through redundancy and task re-allocation. However, a failure that manifests itself in one computer communicating conflicting information to other computers is referred to as a Byzantine Failure, or as a Byzantine Generals Problem.<sup>[12]</sup>

In a distributed computing system, Byzantine failures manifest themselves through errors of omission or commission, rather than total equipment failure. Byzantine failures may occur due to hardware failure, software bugs (register overflow), architecture limitations (propagation of round-off errors among consecutive computations) or malicious attacks. The impact of a Byzantine failure is independent of the cause, allowing us to focus on vulnerability and impact, and disregard the threat at this stage of analysis.

We apply Byzantine failure analysis to estimate the impact of a compromise in information flow across the IEB of a SUT. For example, an incorrect Global Positioning System (GPS) signal to an electric power generator, combined with a hardware failure in an atomic reference clock, may cause an erroneous frequency reference that disconnects the generator from the electric grid.

### ***2.5 Classes of Vulnerability***

Estimating the mission impact of information compromise is by far the most complex step in the cyber risk assessment process. Mission impact may be deterministic in nature, although it may manifest itself in a stochastic or probabilistic manner. The impact of an information compromise may depend on the operational environment of a mission, and certainly on the architecture, specification and implementation of the MEF that uses the compromised information.

A fractal mapping of mission dependence on cyber starts at the IEB of the SUT, showing a block diagram with information ingress and egress. Figure 2. shows a simplified IEB for a notional remotely-controlled aircraft. At the highest logical level, the IEB shows two classes of information exchange: wired when the aircraft is on the ground and wireless during flight. Further refinement may identify wireless communication, GPS signal, LASER ranging and camera.

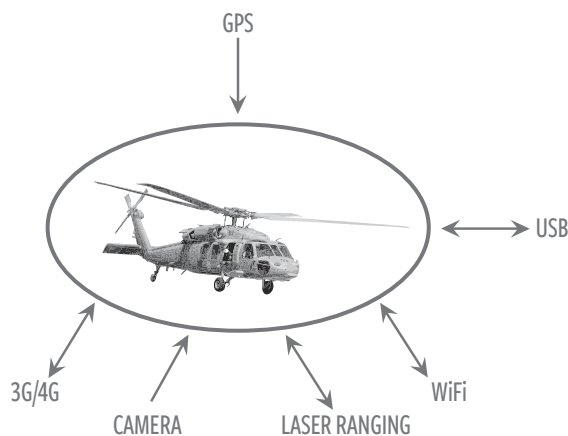


Figure 2. Notional Information Exchange Boundary

A higher fidelity mapping identifies the MEF depending on each of information exchange, outlines the architecture of the MEF, enumerates the specification requirements, and itemizes the details of the implementation. In accordance with our premise that functionality leads to vulnerability, we distinguish among three classes of design features that lead to cyber vulnerabilities:

- i. Architecture vulnerabilities: these result from resource sharing inherent to distributed computer systems, as well as redundancy intended for reliability and safety.
- ii. Specification vulnerabilities: these result from higher-level requirements for specific protocols, data formats, operating systems, authentication schemes, commercial off-the-shelf (COTS) sub-systems, and common standards.
- iii. Implementation vulnerabilities: these include hardware, software and configuration errors.

A systematic information flow analysis that depicts all information generation, processing, communication, storage, consumption and destruction in each critical MEF may reveal inherent vulnerabilities in the architecture, specification and implementation of the MEF.

Subject Matter Experts (SME) with the right engineering education on the fundamentals of the MUT, working in close collaboration with cyber SME educated on the science of information assurance and trained on the art of cyber warfare, provide the minimum skill set necessary to identify the mission impact of a vulnerability to information compromise.

### ***2.6 Blue Book of Cyber Vulnerabilities***

We advocate generating a Blue Book that documents the cyber vulnerabilities in a SUT, coupled with the estimated impact of a Byzantine exploitation of each vulnerability. In addition to enumerating all information exchanges across the IEB of the SUT and detailing the properties of each information exchange, a Blue Book must include a detailed information flow diagram from the IEB into the system, highlighting those sub-systems and components that constitute an MEF, and identifying the potential impact of an information compromise.

The potential impact of a compromise in information integrity and information availability on an MEF does not address the question of a compromise in system authentication. The designer of the Blue Book possesses the latitude to treat compromises in authentication as integrity compromises, or to create a separate class of vulnerabilities that deal with authentication, and potentially non-repudiation.

## 2.7 Cooperative Blue Team Testing

The ultimate objective of a Blue Book is to advise a cooperative Blue Team on the design of tests to validate or repudiate the hypotheses relating information compromises to mission impacts. While we must not mistake the absence of evidence of vulnerability for the evidence of absence of vulnerability, cooperative Blue Team testing seeks primarily to connect vulnerability to impact, independent of threat.

When designing Blue Team test experiments, the testers have unfettered access to the IEB of the SUT. This access permits them to replicate the information compromises detailed in the Blue Book, and observe whether the predicted impacts occur under a representative testing environment. The results of the Blue Team testing serve three purposes. First, they inform the adversarial Red Team on which information compromises to pursue maliciously. Second, they advise the mission owner on cyber risk to the mission. Third, they establish a roadmap for mitigation efforts based on the intent of the mission owner.

## 3. CYBER THREAT CHARACTERIZATION

The success of a cooperative Blue Team in demonstrating the mission impact of an information compromise accounts for two components in the risk equation: vulnerability and impact. The third component, threat, represents the capability—time, talent and treasure—necessary to replicate the impact in an adversarial manner, the access means—remote, physical, supply chain, and the intent—which we assume is there.

While the Blue Team enjoys direct access to the IEB, we elevate the stakes to the Red Team by forcing it to replicate and exercise a realistic threat. Threat characterization is a complex undertaking due to a continuously evolving operational environment driven by new technologies available to both mission owner and attacker, and the insatiable thirst for new capabilities with unforeseen vulnerabilities that expand the attack surface.

While our vulnerability assessment focused on the consequence of an exploit—answering the *what* question, threat characterization focuses on capabilities and means to carry out an exploit—asking the *how* question. Separating Blue Team Testing—the *what*—from Red Team Testing—the *how*—eliminates the constant need for adaptive solutions to test for and mitigate evolving threats, and allows Red Team composition to consist solely of cyberattack experts without the requirement for mission experts.

---

---

Estimating the mission  
impact of information  
compromise is by far  
the most complex  
step in the cyber risk  
assessment process.

We characterize a peer nation state cyber threat by the following attributes:

- a. Highly educated on the science of information assurance
- b. Doctrinally trained on the art of cyber warfare
- c. Adequately resourced in time, talent and treasure
- d. Thoroughly briefed on our target missions and systems
- e. Mathematically specialized in architectural properties
- f. Superiorly skilled in Byzantine failure analysis
- g. Intricately involved in protocol specification and analysis
- h. Critically embedded in the supply chain
- i. Strategically postured in our command and control
- j. Conveniently situated for access and persistence.

As a Red Team of aggressors attempt to understand, replicate and exercise a realistic peer nation state cyber threat, we grade on a scale of zero to ten their success in replicating the above ten characteristics, cautioning against the trap of projecting onto adversaries our way of thinking about cyberattack.

### ***3.1 Cyber Kill Chain***

A United States Air Force (USAF) centric model of air war decomposes the kill chain into the six phases of Find, Fix, Track, Target, Engage and Assess (F2T2EA)<sup>[13]</sup>. This model of the kill chain contains subtle differences from the traditional cyber kill chain that Lockheed Martin introduced in 2011<sup>[14]</sup>, and which consisted of the seven steps

---

We seek to estimate the impact of an information compromise in terms of the D5 effects: disruption, degradation, denial, destruction or deception.

of reconnaissance, weaponization, delivery, exploitation, installation, command and control, and exfiltration/effects.

Both models require access to the target as a necessary step to delivering effects.

While the Blue Team conducting cooperative vulnerability assessment enjoyed access to the IEB, a Red Team replicating a realistic cyber threat must achieve access in an adversarial or malicious manner, and escalate that access into generating D5 effects against the mission. The ten threat characteristics that we outlined earlier provide a realistic challenge, as well as a roadmap, to the Red Team to exploit a mission or system.

We note that access is neither necessary nor sufficient for generating an adverse impact to a mission. On the necessary argument, many cyberattack techniques do not require access to the target system, and have the ability to generate an adverse impact through remote or intermediate components such as man-in-the-middle attacks. On the sufficient argument, access alone to a target system does not guarantee the ability to deliver an adverse impact. This is where testing plays a role in proving or disproving the ability to produce an adverse impact by exploiting a vulnerability.

### ***3.2 Risk Decomposition***

Once a Blue Team demonstrates the impact of a cooperative information compromise, the job of the Red Team boils down to replicating that information compromise in an adversarial manner. Risk decomposition reduces the mission-specific engineering expertise required of the Red Team, and limits the required skill set to cyberattack against critical information. This deliberate distinction between a Blue Team of mission SME and a Red Team cyber SME places the mission owner at a significant advantage against an adversary who must demonstrate combined mission and cyber expertise. The end product of Red Team testing is a Red Book documenting validated threat replication to exploit the vulnerabilities identified in the cooperative Blue Book.

---

---

Estimating the mission  
impact of information  
compromise is by far  
the most complex  
step in the cyber risk  
assessment process.

### ***3.3 Modeling and Simulation***

Modeling of modern complex information systems and simulating their operation provides both Blue Team and Red Team a safe environment to validate and verify the perceived impact of information compromises. However, modeling and simulation (M&S) suffers from the limitation of the user perception of how a system must behave, rather than how it behaves in the real world. In many instances, partial differential equations with no exact solution model the real world, and many simulators enforce desired properties and behaviors that fail in the real world. If a model designer chooses wrong parameters or makes trivializing assumptions, simulation gives incorrect results.<sup>[15]</sup>

Defense Acquisition University (DAU) defines Validation, Verification & Accreditation (VV&A) as the process of determining that a model or simulation implementation and its associated data accurately represent the developer's conceptual description and specifications (verification); the process of determining the degree to which a model or simulation and its associated data accurately represent the real world from the perspective of the model's intended uses (validation); and the official certification that a model or simulation and its associated data are acceptable for a specific purpose or use (accreditation). DoD



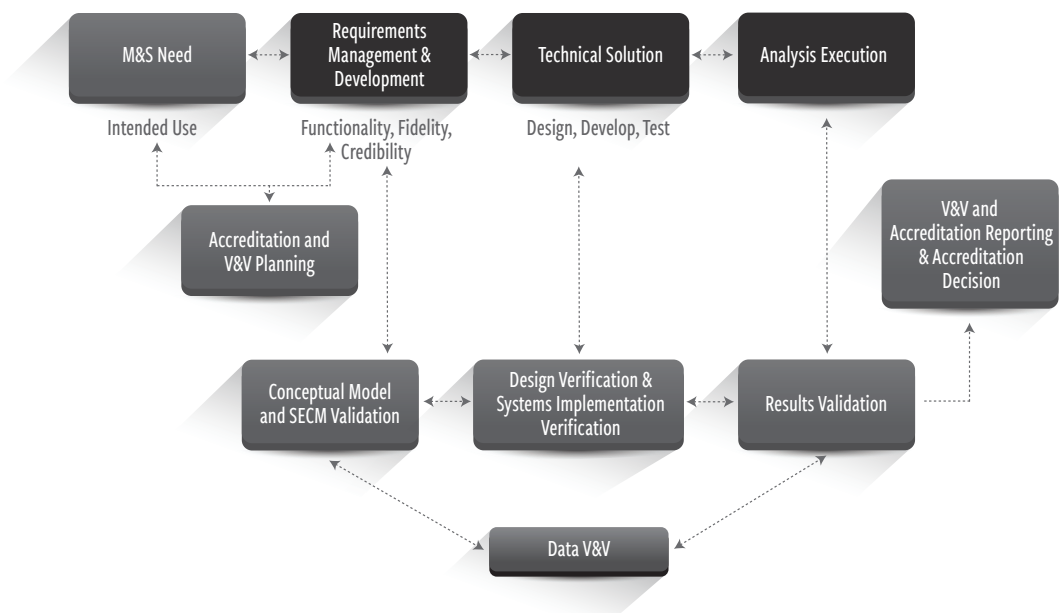


Figure 3. DoD representation of Validation, Verification and Accreditation Approach Process

Instruction (DoDI) 5000.61 mandates the use of the VV&A process as part of any M&S-based solution to risk assessment of defense systems. Given its predominantly compliance-based approach, VV&A falls short of increasing the fidelity of impact estimation of cyber vulnerability.

#### 4. TESTING

Testing presents an opportunity for a cooperative Blue Team and an adversarial Red Team to act as trusted agents and honest brokers advising commanders on cyber risk to critical missions and systems, and identifying areas for S&T insertion in both the test process and vulnerability mitigation, and informing subsequently the development of future systems.

##### 4.1 Cooperative Blue Team Testing

Following the identification of a potential vulnerability to information integrity compromises and the resulting mission impact, Blue Team testing seeks to validate such a hypothesis. We view the members of a cooperative Blue Team as mission experts schooled in the technology and engineering of the MEF. This *knowledge of us* approach seeks to answer the *what* question—what is the mission impact of a compromise in the integrity of information entering or exiting the IEB of the MUT.

Blue Team testers enjoy unfettered access to the MUT, allowing them to inject bad data

into the MUT through the IEB. The goal of the Blue Team is to estimate the impact of accidental or intentional information compromise in terms of disruption, denial, degradation or destruction of the mission, or deception. By applying Byzantine failure analysis to information flowing across the IEB, as well as information flowing among components within the IEB, we focus Blue Team testing on consequence independent of cause.

The set of all the vulnerabilities whose exploit results in adverse impacts to the mission makes up the vulnerability surface. The testing literature uses attack surface interchangeably with vulnerability surface, both terms referring to characteristics and properties under the control of the mission owner.

#### ***4.2 Adversarial Red Team Testing***

Since the cooperative Blue Team focuses on assessing the mission impact of vulnerability exploitation—the *what*—the Red Team seeks to effect this exploitation through adversarial means—the *how*. Segregating the roles of the Blue and Red Teams allows building highly qualified Blue Teams of mission SME with limited cyber expertise, and conversely highly qualified Red Teams of cyber SME who lack mission expertise.

Once the Blue Team quantifies the impact of a cooperative information compromise, the job of the Red Team becomes to effect the same information compromise in a malicious manner. A Red Team of information aggressors develops the knowledge of them—understand the threat, replicate the threat, exercise the threat. The threat knowledge includes adversary capability in terms of time, talent and treasure, as well as attack means and intent.

A validated threat against a known vulnerability constitutes an attack vector, with the origin of the vector in the adversary camp and the destination in the mission camp. The total set of validated threats against identified vulnerabilities form the attack vectors.

We quantify in terms of talent, time and treasure the adversary capability necessary to compromise an information flow leading to the exploit of a vulnerability with an adverse mission impact. The talent of a realistic nation state adversary includes formal college education on the science of information assurance and extensive doctrinal training on the art of cyber warfare. The time element of the threat refers to the planning necessary to exploit a vulnerability, including the intelligence preparation of the environment for successful exploitation. Treasure refers to the cost in manpower and resources for successful exploitation, such as computing power to break passwords by brute force.

The attack means include the required tools to complete the attack kill chain, including access, persistence, generating effects and conducting damage assessment. Access may be remote over the Internet, local through physical access, supply chain of software or hardware, or access-less through man-in-the-middle attacks.

Traditional threat estimation considers the likelihood of a threat as a function of capability, access and demonstrated intent. For cyber risk assessment purposes, we assume intent given capability and access. In other terms, we exclude the qualitative assessment of intent from the quantitative estimate of threat, and consequently risk.

Lastly, we must ensure that the Red Team of aggressors understand, replicate and exercise a realistic cyber threat, not the projection of our idea of what the threat ought to look like. The USAF and the Lockheed Martin models of the kill chain reflect a narrow concept of how cyberattacks should be conducted, and falls woefully short of an accurate reflection of the global cyber threat environment. We must also ensure that we look at not just the current threat, but the projected threat across the lifecycle of the system under test.

## 5. MITIGATION STRATEGY

Mitigation seeks to reduce the risk to a mission by manipulating both ends of an attack vector: reducing vulnerability and increasing the cost to a threat, while reducing the potential impact of a successful exploitation. We observe one key lesson learned from safety investigation of aviation mishaps: to prevent a recurrence of a serious mishap, safety investigation reports recommend materiel solutions to augment plausible changes in tactics, techniques and procedures (TTP).

Many in the network security community seek to train users not to open attachments, click on web links or insert thumb drives into computers. In the meantime, several companies introduced materiel solutions that can mitigate the vulnerability of user actions, where training and TTP alone have failed.

One of the mitigation challenges of critical missions is the tradeoff between integrity and availability. It is often easier to assure a mission against the loss of available resources, but a lot harder to assure against covert compromises in information integrity.

Mitigation follows the normal sequence of vulnerability assessment, threat estimation, testing and mitigation, and represents the culmination of the mission assurance process. When Blue Team testing validates the hypothesis of mission impact of an information compromise and Red Team testing validates adversary capability to exploit such vulnerability, mitigation seeks to eliminate the vulnerability or reduce its impact, while increasing the cost of adversary exploitation.

We advocate a three-phase approach to vulnerability mitigation: TTP where practical, materiel solutions to augment or enforce TTP, and the pursuit of S&T solutions when no materiel solution exists. It is important to note the role of cyber security in vulnerability mitigation. While firewalls and virus scanners may play a role in mitigating configuration vulnerabilities, they often fall short in mitigating architectural and specification vulnerabilities, and may create additional vulnerability that increases the attack surface.

### ***5.1 Tactics, Techniques and Procedures***

One might argue that TTP are the tactical extension of strategy and policy, and that a disconnect between cyber policy and technology presents a threat to corporate and national security. Consequently, regulators and mission owners may increase the risk to their missions through policies and the resulting TTP. Having said that, not all TTP are ineffective. The Bell-LaPadula Model of access control<sup>[16]</sup> protects information in a multilevel security system through a policy that prohibits “reading up or writing down.” Failure to enforce this fundamental TTP enabled well-publicized breaches of classified information.

In complex distributed computing systems, we view the role of TTP as mitigating vulnerability caused inadvertently by policy and guidance. For example, a measure or policy that applies equally to *all information systems* may ignore the different impacts of information compromise of a national security system versus an IT office automation system, and may require TTP to distinguish between these two classes of impacts.

---

---

One of the mitigation challenges of critical missions is the trade-off between integrity and availability.

Similarly, policies that trade away security for convenience, efficacy for efficiency, quality for cost, and integrity for availability, have an adverse effect on mission risks. Lastly, common misconceptions in cybersecurity practices mistake monitoring for defense, absence of evidence for evidence of absence, detection for protection, and projection for prediction.

### ***5.2 Materiel Solutions***

When reversing harmful policies and TTP fall short of mitigating cyber risk to a mission, disruptive materiel solutions may mitigate vulnerability. We provide several examples to illustrate our point, but we caution against viewing them as universal solutions looking for problems.

Quantum sensing and quantum communication eliminate the vulnerability of radio frequency (RF) transmission to eavesdropping, information manipulation or information spoofing. Read-Only Memory (ROM) reduces the vulnerability of a piece of software to accidental or malicious modification. Different size nozzles reduce the likelihood of diesel fuel filling a gasoline tank.

For supply chain management, split fabrication of integrated circuits provides a disruptive paradigm to reduce the risk of malicious backdoors in hardware, at significantly lower cost and higher potential success than detection.

### ***5.3 Science & Technology***

In cyber risk management, mathematics is the friend of the defender and the nemesis

of the attacker. The Rivest-Shamir-Adelman (RSA) Cryptosystem for public key cryptography<sup>[17]</sup> provides a compelling example. The difficulty in factorizing the product of two very large prime numbers provides the strength to the algorithm. The computational cost of multiplying two numbers will always be lower than the cost of factorizing the resulting product. Mathematical specification of the security requirements of a function allows the formal verification that the eventual implementation satisfies those requirements. In theory, this approach may yield an error free, vulnerability free, unhackable implementation. In practice, we can increase disproportionately the cost to a threat, and reduce the impact of an exploit.

The proliferation of cloud computing and its benefits in cost and redundancy drive the research on trading off information availability for information integrity. Mitigating cyber vulnerabilities caused by MEF architecture and single points of failure lead inevitably to public cloud computing, raising the traditional IA issues of confidentiality, integrity and availability. Atomic computing—where a computation either completes or does not—combined with homomorphic encryption<sup>[18]</sup>—where functions can operate on encrypted data and yield encrypted results—can guarantee trust and integrity of a completed transaction, but not its availability. Implementing national security missions in public clouds with some form of homomorphic encryption provides S&T challenges and fascinating prospects that deserve thorough study.

## 6. NOTIONAL CASE STUDY

In this section, we bring together the concepts of risk assessment, testing and mitigation into a notional case study. We examine the cyber risk to the mission of a Remotely Piloted Aircraft (RPA) used for power line inspection.<sup>[19]</sup> The vast expanse of High Voltage (HV) power transmission lines makes them vulnerable to inclement weather. HV lines are particularly susceptible to lightning, and their design provides circuit breakers and fuses to prevent propagation to generators and transformers. Regardless of the built-in protections, lightning may damage the insulators that hold mechanically the lines to the towers. Visual, infrared and RF inspection may detect electrons leaking at the periphery of a damaged insulator. This leakage generates a corona effect, predictive of a likely catastrophic failure. Therefore, inspecting HV transmission lines following a thunderstorm has become a prudent preventive practice in the industry.

### ***6.1 Helicopter Characterization***

The JR GSR260Z is a gas-powered remote controlled helicopter with a 26cc engine that provides the power to carry an 11lb payload. Depending on the payload, a full tank of gas provides up to 30 minutes of flight time with a range of 10 miles. A recent demonstration in Eastern Finland used the following helicopter configuration:

- ◆ Aircraft: JR GSR260Z, combustion engine
- ◆ GPS receiver: NEO M8N
- ◆ Doctrinally trained on the art of cyber warfare
- ◆ Take-off and landing controlled by manual controller
- ◆ Actual flight piloted by autopilot using GPS satellite navigation information.
- ◆ Real time video for flight control 720p IR camera
- ◆ Surveillance camera: Sony  $\alpha$ 7R, 36.4 megapixel full area ( $35.9 \times 24$ mm) CMOS image sensor, objective 70mm zoom, firing control via autopilot. Memory card 128GB SDXC
- ◆ LIDAR: Hokuyo UXM-30LXH-EWA for vegetation and clearance analysis
- ◆ Control communications: 16 channel radio controller and 3G/4G public mobile networks
- ◆ Mission Planner GCS open source software for mission planning
- ◆ Finnish basic land maps and Google maps

## ***6.2 Mission Decomposition***

We decompose the mission of the JR GSR260Z into the following MEF:

- i. take off and navigate to the power line
- ii. achieve stable flight over the target with positive control by the operator
- iii. establish a reliable return video feed from the RPA to ground control
- iv. store surveillance video on internal SD card for further processing
- v. land safely at the end of the mission.

We make the following assumptions to bound the solution space for this case study:

- i. no onboard processing of the video surveillance signal for damage identification
- ii. autonomous flight operation in areas with weak 3G/4G cellular signal
- iii. GPS waypoint return home feature in the event of Command and Control (C2) loss.

## ***6.3 Test Design***

Figure 2. depicts a notional information exchange boundary. We analyze the mission impact of a compromise of two information exchanges, namely the GPS and the 3G/4G cellular signal.

If GPS signal availability is compromised by nearby mountains that block satellite signals or parasitic electromagnetic interference from electric power equipment that result in a jamming effect, direct operator C2 of the aircraft permits successful mission accomplishment.

The loss of 3G/4G cellular communication due to the absence of nearby cell towers can be mitigated through GPS waypoint navigation augmented by automatic power line tracking via pattern recognition of the navigation camera.

The simultaneous loss of both GPS signal and 3G/4G signal denies the aircraft the ability to complete the mission of recording surveillance video, and may even result in the destruction of the aircraft.

Given the hypothesis of the vulnerability of the mission to compromises in the availability of GPS and 3G/4G information flows allows the design of a cooperative Blue Team testing. Turning off the GPS and the 3G/4G cell phone in a controlled flight environment demonstrates the desired impact.

On the Red Team side, estimating the adversary capability necessary to deny the two signals leads to considering jamming signal directed against the aircraft. However, a priori knowledge of the 3G/4G communication protocol may permit a man-in-the-middle attack (such as temporary jamming) to drop a connection, and substitute it with a rogue connection that can divert or destroy the aircraft. Similarly, an attack on the integrity of the GPS signal through spoofing may have similar consequences.


#### ***6.4 Vulnerability Mitigation***

A sample materiel solution to mitigate the vulnerability of simultaneous loss of GPS and 3G/4G cellular signals involves electro-optical and infrared (EO/IR) navigation. If the aircraft carried on board adequate computing capability, alternative navigation means may become possible. For example, storing video footage of the terrain under examination, an EO/IR navigation algorithm permits accomplishing the mission of recording surveillance video of the area under test, and successfully returning to base, even in the absence of GPS and 3G/4G signals.

### **7. CONCLUSION**

We presented a systematic top-down approach to identifying cyber vulnerabilities in a complex information system through a disciplined information flow analysis, and estimating the mission impacts of information compromise. We applied Byzantine failure analysis to separate the impact of an information compromise from the underlying cause of the compromise, whether accidental or malicious. We advocated generating an introspective Blue Book of cyber vulnerabilities at the end of this vulnerability assessment phase to guide the cooperative test activities by a Blue Team. The subsequent development of a Red Book sought to quantify adversary capabilities necessary to exploit the cyber vulner-

abilities that the Blue Book identified. The Red Book provided Red Teams with a roadmap to conduct adversarial testing by a Red Team, and defined the threat capabilities that an aggressor team sought to understand, replicate and exercise.

We completed our discussion of mission assurance by addressing vulnerability mitigation. We explored first TTP where applicable, discussed materiel solutions when TTP fell short, and advocated the pursuit of S&T solutions. We concluded the paper with a notional case study. 

*The views expressed are those of the author and do not reflect the official policy or position of the Air Force, Department of Defense, or the U.S. Government.*

*Product names are trademarks of their respective owners. Mention of product names does not constitute endorsement by the United States Air Force, the Department of Defense, or the U.S. Government.*



## NOTES

1. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, NIST Special Publication 800–30, July 2002.
2. Guide for Conducting Risk Assessments: Information Security, National Institute of Standards and Technology, NIST Special Publication 800–30-rev1, September 2012.
3. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 8 November 2010 (As Amended Through 15 November 2015).
4. DoD Policy and Responsibilities for Critical Infrastructure, Department of Defense DoD Directive 3020.40, July 2010.
5. Cyberspace Operations, Air Force Doctrine Document AFDD 3-12, 15 July 2010, Incorporating Change 1 30 November 2011.
6. Department of Defense Architectural Framework, DoDAF version 2.02, 2011.
7. The Defense Acquisition System, Department of Defense Directive 5000.01, 12 May 2003.
8. Operation of the Defense Acquisition System, Department of Defense Directive 5000.02, 12 May 2003.
9. Test and Evaluation Overview, Defense Acquisition University, Lesson 18, 2006.
10. The Science of Mission Assurance, Dr. Kamal Jabbour and Dr. Sarah Muccio, Journal of Strategic Security, Volume IV Issue 2 2011, 61-74.
11. On Mission Assurance, Dr. Kamal Jabbour and Dr. Sarah Muccio, Conflict and Cooperation in Cyberspace: The Challenge to National Security, Editors: Panayotis A. Yannakageorgos and Adam B. Lowther, Taylor Francis CRC Press, 21 July 2013.
12. The Byzantine Generals Problem, Leslie Lamport, Robert Shostak and Marshall Pease, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, 382-401.
13. Deterrence in Cyberspace, Dr. Kamal Jabbour and E. Paul Ratazzi, Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century, Editor: Adam B. Lowther, Palgrave Macmillan, December 2012.
14. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Hutchins, Cloppert, et al. Lockheed Martin Corporation, 2011, 4-5.
15. On the Partial Difference Equations of Mathematical Physics. Courant, R.; Friedrichs, K.; and Lewy, H. IBM J. 11, 1967, 215-234.
16. Secure Computer Systems: Mathematical Foundations, David Elliott Bell and Leonard J. LaPadula, MITRE Corporation, 1973.
17. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Ronald Rivest, Adi Shamir and Leonard Adleman, Communications of the ACM 21 (2): 120–126, February 1978, 120-126.
18. Fully Homomorphic Encryption Scheme, Craig Gentry, PhD Dissertation, Standofrd University, 2009.
19. Demonstration of Unmanned Aircraft for Powerline Inspections, Ville Koivuranta, LiDAR News Magazine, Vol. 5 No. 2, 2015.

# Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations

---

Dr. Jan Kallberg

## INTRODUCTION

Each strategy has a foundation—an overarching way of explaining why things are the way we see them, and how to successfully reach our goals. Therefore, strategy is theory-based because theory provides an intellectual framework for predicting outcomes leading to the end goal the strategy pursues. This article will present the strategic cyberwar theory whose utility is tied to the likelihood of institutional instability in the targeted nation. In an ideal scenario, a nation conducts systematic cyber attacks against the targeted adversary's institutions triggering the dormant entropy embedded in a nation possessing weak institutions. This will lead to submission to foreign will and intent.

This framework will change the way nations view cyber. It is no longer an enabler for joint operations, but instead a strategic option to confront adversarial societies. The current alternative to strategic cyberwar theory is to unsystematically attack the adversary with cyber attacks where exploitation opportunities occur, which is likely to degrade parts of the information infrastructure, but will not attain any strategic goals. If an adversarial society is unaffected by a cyber conflict, the conflict itself has not reached a decisive outcome, and results in a *tit-for-tat* game or stalemate. Decisive outcome must lead to policy change as a partly or full submission to foreign will by the targeted society. The decisive cyber outcome is either reached by removing military capacity through cyber attacks or destabilization of the targeted society. The removal of military capacity is likely temporary, followed by software coding to close these limited vulnerabilities, compared to a societal destabilization that jeopardizes the regime.

In strategic cyberwar theory, attacking the adversarial nation's institutional framework will result in destabilization. If a nation is destabilized, it can be subdued to foreign will, and the ability for the current regime to execute their strategy evaporates due



Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham.

Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is [www.cyberdefense.com](http://www.cyberdefense.com).

to loss of internal authority. The theory's predictive power is strongest when applied to targeting theocracies, authoritarian regimes, and dysfunctional experimental democracies, and their common tenet of weak institutions.<sup>[1]</sup> Fully functional democracies, on the other hand, have in cyberwar a definite advantage because advanced democracies have stable and accepted institutions. Nations openly hostile to democracies are in most cases totalitarian states that are close to entropy. The reason these totalitarian states maintain their power is through suppression of the popular will. Any removal of the pillars of suppression will destabilize the regime design and key institutions that make it functional, and could release the popular will. A destabilized and possibly imploding Iranian regime is a more tangible threat to the ruling theocratic elite than hacked military information subsystems. Dictators fear the wrath of the masses.

Strategic cyberwar theory looks beyond the actual digital interchange, the cyber tactics, and instead creates predictive power of how a decisive cyber conflict should be conducted in pursuit of national strategic goals.

### ***The Need for Cyber Theory***

Theory is an overarching way of combining ideas, phenomena, and facts, in a generalized form, to seek to explain specific outcomes. Theory's strongest tenet is predictability. Theory can serve as guidance to prepare for future events and ensure these outcomes are favorable. Theories are created to better understand the world. As an example, the democratic peace theory,<sup>[2][3]</sup> asserts that democratic states do not fight each other, and therefore the theory predicts citizens on both sides of the Saskatchewan and North Dakota border should not fear the imminent risk of a military invasion.

In a militarized Internet, it is convenient to rely on traditional military theory transposed into cyber.<sup>[4]</sup> It works as an intellectual short cut, but the traditional military thinking fails to acknowledge the unity tenets of cyber. Traditional military theory applied to cyber conflict has four challenges: anonymity, object permanence<sup>[5]</sup>, measurable results, and rapid digital execution. In a Clausewitzian world, these challenges were non-existent. First, the enemy was clearly identified; a state of war was declared; a French Napoleonic general overlooking the battle could clearly distinguish a thin red line of British troops waiting for the advancing French Guards in blue uniforms. There was a basic understanding of who were the parties in the conflict, their past actions, and the strategy that drove their action. Next challenge for traditional military strategy is object permanence. The general could march its armies to a point where the next day the battle is joined with a map laying out his course of action. The landscape would be intact the next day, the roads had not moved, and the hills stood where they should. If there is no object permanence, maneuvering concepts<sup>[6]</sup> become irrelevant because maneuver increases the opportunity for success, and if we are unable to relate in time and space, maneuvering is nullified. The third challenge is quantifiable results. The French Napoleonic general storming the thin red line of British troops could see with his own eyes how the line of British troops became thinner and thinner following each rifle volley. The French general would receive an accurate measurement of effectiveness in real time, forcing a retreat if the British were still standing after the French Guards lost their battlefield thrust. Measurable results are needed as information for further decision-making and battle assessment.

Cyber lacks the feedback loop of quantifiable results and with limited measure of effectiveness. The next move in traditional military theory relies on a chain of events leading to a decisive moment. Computers at war do not engage at human speed, the engagements occur at computational speed. Even if we solved the challenges of anonymity, the lack of object permanence and the absence of measurable results, computerized machine speed in which premeditated systematic cyber attacks would eradicate any influence of human leadership. In reality, the cyber attacks would be over before any leadership understood the strategic landscape. If the attacks were not premeditated, but relied on harvesting vulnerabilities in an ongoing conflict, the time frames in which larger future engagements could occur limits, or in worst case nullifies, the ability to orchestrate the cyber defense. The uniqueness of cyber removes the predictive power of traditional military strategy.

---

---

If an adversarial  
society is unaffected by  
a cyber conflict, the  
conflict itself has not  
reached a decisive  
outcome, and results  
in a *tit-for-tat* game  
or stalemate.

### *Going from the Unknown to the Known*

If battle results cannot be quantified, there is no object permanence, and the assumed enemy is anonymous, and the battle occurs at computational speed; any grander battle strategy is becoming inferences about the unknown. Strategic cyberwar theory<sup>[7]</sup> utilizes the thinking of Bertrand Russell in his version of Occam's razor: "Whenever possible, substitute constructions out of known entities for inferences to unknown entities."<sup>[8]</sup> Occam's razor is named after the medieval philosopher and friar William of Ockham who stated that in uncertainty the fewer assumption the better and pursuing simplicity by relying on the known until simplicity could be traded for greater explanatory power. The following statements are basic knowledge with limited uncertainty.

Societies are engaged in conflicts. The cornerstone for any society is institutions. The institutional resilience varies by nation, from stable democracies to totalitarian states on the brink to entropy. The destabilization effort needed to impact the whole society must have an intensity reaching beyond the targeted nation's resiliency.

If institutions fail, society will be destabilized and weakened. A destabilized society collapses or is subdued to foreign power. These above statements are established common knowledge in political science, and act as a stated known. Following the stated known,

Fully functional democracies, on the other hand, have in cyberwar a definite advantage because advanced democracies have stable and accepted institutions.

strategic cyberwar theory seeks to explain how an adversarial society can be destabilized and subdued by a major cyber campaign. Cyberwar has to be quickly executed, shocking the targeted society, and at the same time avoid adaptive behavior that mitigates the damages from

the attacks. The rapid execution denies the targeted nation the opportunity to create defensive measures and eliminate any possibility to strategically lead a coherent cyber defense.

A cyber attack will fail to destabilize the targeted society if the institutions remain intact following the assault or operate in a degraded environment. Therefore it is important to ensure the cyber attack is of the magnitude that forces the targeted society over the threshold to entropy.<sup>[9]</sup>

### *The Future Cyberwar*

Within the first two decades of the Internet, the public discourse regarding cyberwar has injected digital fear and belief that everyone is vulnerable to cyberattacks. The initial view stressed that limited options were available to prevent cyberattacks<sup>[10]</sup>, generating a

cyber-Pearl Harbor hysteria,<sup>[11][12]</sup> juxtaposed with the belief that cyberwar was unlikely to happen.<sup>[13]</sup>

The positional underpinning that cyberwar is unlikely is based on the premise that its impact would not reach the threshold of war. Thomas Rid, and other proponents of this concept focus their analysis on unsystematic attacks with modest complexity. These simple intrusions exploit single digital opportunities, such as theft of data or marginal system disruptions, instead of seeking geopolitical objectives. One of Rid's main arguments is that cyberwar has never reached the Clausewitzian threshold of war. What is war in a Clausewitzian *weltanschauung*? According to Clausewitz, the purpose of war is to conquer and destroy the armed power of the enemy, take possession of its material and other sources of national power, and gain public approval.<sup>[14]</sup> Cyber does not want to possess, as stipulated in Clausewitz's definition, so according to the Clausewitzian definition it fails to meet the definition of war. The absence of actual casualties, or similar destruction in cyberwar is a result of what is considered a cyberwar. A set of sporadic denial of service attacks on social media will naturally not reach the threshold for cyberwar, but destabilization of a regime utilizing cyber will subscribe to the definition of war. It is a perpetrated and intended attack on a nation state in pursuit of removing authority and control, which can in dormant entropies trigger civil war, regime collapse, and (or) violent regime shift.

The notion that cyber cannot be a tool for war is itself dated and naive. The recent entrance of state actors as heavily engaged cyber perpetrators changed the earlier cyber attack paradigm of unfunded individuals hacking into systems because they saw the opportunity to do so, and moved it to a new set of goals and intents that are aligned with the interests of the state actor.<sup>[15]</sup> The focus on the lower levels of digital interchanges has colored the debate about future cyberwar.

The international community has not witnessed a cyberwar, but instead view anecdotal digital interchanges that serve limited state interests. The Mutual Assured Destruction (MAD) theory of nuclear deterrence works well without any mutual destruction having occurred. The absence of past events does not remove the likelihood of future occurrence. If that was true—the claim that cyberwar will not happen because it has not happened—then a nuclear missile interchange would be impossible in the future because there are no past events.

### ***Competing Cyber Strategy Thoughts***

The strategic cyber discourse in recent years has a limiting central theme that cyber can only support and enable existing military and geopolitical operations. This core argument views cyber purely as an enabler for joint operations in the absence of a successful cyber-heavy conflict. The cyber theorizing paradigm refuses to acknowledge the oppor-

tunity for decisive cyber capabilities in 30 to 40 years, and instead, base their analysis on current capacities, and focus on marginal effects of unstructured, mainly simplistic, and sporadic cyber attacks. Path dependency<sup>[16][17]</sup> and tradition<sup>[18]</sup> should not blur or remove the strategic lenses in which we see the opportunity cyber brings. The risk of seeing the cyber world emerging as a mechanical part of the environment assumes that it is submerged and will not change. The trap that is created by path dependency and tradition can be presented by another word—assumption.

The main risk in the current cyber discourse focuses on cyber as purely an enabler of joint operations. This is featured in numerous assumptions, and a product of traditional burdened perceptions:

1. lacking understanding of the reversed asymmetry of the conflict, where a state can attack a domestic public entity and individual citizens,
2. ignoring the absence of object permanence,
3. the belief that cyber conflicts solely will be a match between military networks,
4. that digital interchange is conducted according to our concept of ethics and norms,
5. absence of acceptance of the rapid time frame interchanges will occur,
6. reliance of non-existent measure of effectiveness (MOE),
7. weak comprehension of the imminent future's automated computational speed conducted harvest of vulnerabilities and execution of attacks, and
8. the impact of artificial intelligence in combination with automated harvest of vulnerabilities.

If cyber warfare is limited to enabler status, other operational intent will drive the execution towards the strategic goal. Cyber capabilities offer a strategic opportunity that will grow in coming decades. Cyber effects will be limited if subordinated to enabler status, and by doing so provide democracies reduced military options.

Analogies with nuclear warfighting capabilities have striking similarities with cyber, such as both cyber and nuclear weapons share the power of projected uncertainty. According to Kenneth Waltz, it is not what you do, but instead what you can do that gives you the power.<sup>[19]</sup> Cyber and nuclear weapons both have global reach with minimal ground presence. These similarities are more shared characteristics than strategies. On the other hand, legal theories offer no direct guidance on how to fight in the cyber domain, but instead provide numerous restrictions.<sup>[20]</sup> Law is a codification of political thinking dealing with current issues, but lacks predictive theoretical power.



### ***Cyber: Enabling Tool or a Way to Fight?***

Colin S. Gray argues that cyber power is first and foremost enablers of joint military operations.<sup>[21]</sup> Secondly, Gray asserts that a cyber offensive will not be lethal enough to have a major military impact. Third, cyber is information and information can be ignored. Gray's fourth conclusion is that the wide-spread fear for a stand-alone cyber Armageddon is not logical because it is unlikely to happen. Martin Libicki<sup>[22]</sup> agrees with Gray, and argues that cyber is not a stand-alone mechanism to fight a conflict, but instead an enabler, and he struggles to see cyber as anything else than attacks on computer and networks. Libicki states; "A cyber attack carried out against our military can, at worst, return it to its pre-networked condition."<sup>[23]</sup> The weakness in Libicki's argument is that he assumes cyber conflict would be a military-against-military engagement. It is reasonable to posit that western cyber attack might be restrained, and aimed at exclusively military targets, but nothing ensures that an attack launched by a totalitarian state will obey democratic moral codes, normative ethical values, and restraints. The notion that a future cyber attack will occur in a controlled environment within the realm of old school 'fair play' is specious and generates false security.

The arguments presented by Gray and Libicki might be relevant in the snapshot of today, but these arguments are burdened by tradition, and a part of a larger time-bound context. Logically, it is likely that cyber capabilities will radically progress from this point in time.

#### ***Strategic Cyberwar Theory***

If nation states seek to conduct decisive cyberwar, it will not be achieved by anecdotal exploits, but instead by launching a systematic destabilizing attacks on the targeted society. In strategic cyberwar theory, the intellectual works of Dwight Waldo, a leading political scientist and theorist for over 50 years, are utilized. Waldo studied the theoretical underpinnings that maintain government institutional sustainability and stability. Strategic cyberwar theory turns these theories upside down to create entropy and destabilization. This systematic approach seeks to use institutional weaknesses, popular sentiment, and underlying opposition to the targeted government as force multipliers to the effect. Cyber targeting can induce a sense of lack of control with citizens blaming the state for failing to safe-guard the societal structure.<sup>[24][25]</sup> A nation, or any society, is organized through institutional arrangement, and this requires a set of basic functionalities to operate and ensure continued stability and functionality. Institutions make a state stable, a government sustainable and functional, even in a degraded environment.

---

---

Cyberwar has to  
be quickly executed,  
shocking the targeted  
society, and at the  
same time avoid  
adaptive behavior  
that mitigates the  
damages from  
the attacks.



A systematic institutional cyber attack can be visualized as the collapse of a building built with prefabricated elements, such as a parking garage, or a framework of concrete beams, pillars and decking. If pressure is distributed evenly over the construction there is no risk of collapse and the building is safe. If instead the energy is concentrated on one or a set of the bearing elements, the building will collapse. Waldo's theoretical work outlines what makes a nation state stable.<sup>[26][27]</sup> The strategic cyberwar theory turns Waldo's accepted theories upside down, so instead of upholding the functionality of the targeted society, it seeks to swiftly destabilize the state. Waldo focused his theoretical work on five factors that uphold and stabilize a society: legitimacy, authority, knowledge management, bureaucratic control, and confidence. Authority could then be external authority, by leading or in some cases suppressing a people, and internal authority within the bureaucracy and political structure.

### ***Waldo's Five Pillars for Societal Stability***

Waldo's five factors summarize the pillars of all societies and governments. If a major cyber attack can undermine these pillars, the targeted state is weakened and risks implosion. Legitimate government must be legally legitimized, and capable of delivering the 'good society' or in a dictatorship 'acceptable society'. Legitimacy is a sliding grayscale and cannot be seen as a value that the society either has or not.<sup>[28]</sup> Authority is the ability to implement policy, and in a democracy, it requires the rational acceptance of people, expectations of public good, ethics, and institutional contexts. Institutional knowledge is the ability to arrange and utilize awareness and expertise within the bureaucracy since coordination is always the major challenge. Control is the ability to dominate and have authority over a bureaucracy. Confidence is the trust people have that government delivers the expected benefits and removes that fear of an uncertain future.

These five factors are the framework that hold a government together. If depleted or removed, the absence of the factors will mortally wound a government. In strategic cyber warfare it is pivotal to attack and eliminate one or all of these pillars, which will lead to the collapse or serious damage of the targeted state.

#### ***A. Legitimacy***

Legitimacy concerns not who can lead but who can govern. Waldo believed that citizens need faith in government; for government to have legitimacy, they must promise and then deliver a better life for its citizens. For a major cyberattack seeking to damage state legitimacy, it has to darken the future for the population, and create an assumption that the leadership is unable to govern the country.

#### ***B. Authority***

Authority in totalitarian regimes can be summarized as acceptance for the moment.

Authority and hierarchy are linked when the structure determines the jurisdiction of a specific position. If there is no hierarchy, there is no leadership that can be held accountable for its actions; with no accountability, any organization could fall into entropy and anarchy.

### ***C. Institutional Knowledge***

One of the major challenges for modern government is knowledge management. If public administrators are unable to organize knowledge and information, the citizens are left with the impression the government is incompetent. This is an indirect challenge to authority and could lead to societal entropy. The modern society generates overwhelming amounts of information at all levels, with much of it available over the last two decades. Knowledge is generated by agencies and the public sector through documents, actions, inquiries, publications, and policies. The increase of knowledge requires specialization, according to Waldo, but with specialization comes the challenge to coordinate the information. If a lack of knowledge and coordination affects citizens, it undermines their perception of how well government is working. Cyber attacks on institutional knowledge management will cripple the bureaucracy and anger the population.

### ***D. Bureaucratic Control***

Complex organizations have challenges with a growing bureaucracy. Control can also be lost due to the ineffective coordination among agencies, local and state governments, and other stakeholders. When a government does not have proper bureaucratic control across organizations, jurisdiction is lost. As bureaucracy expands, so do the control issues since control requires coordination. Control issues also arise through unintentional errors. If control is lost, corruption, favoritism, public theft, and popular discontent will follow.

### ***E. Confidence***

Waldo asserted that when people feel secure, they have confidence, and are optimistic about the future; they trust government will provide necessary support. Confidence for Waldo was trust in government to deliver the society it promised. Confidence means the future is perceived to be brighter than the past; legitimacy and authority is defined in the present, confidence is forward-looking. Current global events of scarcity and competition for public resources is harmful to confidence in government, because it challenges future ability to serve citizens. Signs of systematic failure will harm the citizenry's ability to maintain confidence in government.

---

---

The international community has not witnessed a cyber-war, but instead view anecdotal digital interchanges that serve limited state interests.

### *Examples of Targeting*

Strategic cyberwar theory predicts the weaknesses of targeted governments, and assists in remotely initiated regime shift or submission to foreign power. These weaknesses are identified in each society based on the societal characteristics and tenets. Once the weaknesses are identified they are aligned with the theory and operationalized to targeting. The attack in these sectors is likely unexpected by the targeted nation, its cyber defense is defending other sectors of the society, and will initially create turmoil and confusion. These targets selected by strategic cyberwar theory differ in several cases from the traditionally prioritized assets for national cybersecurity and information assurance, such as military, defense-industrial, diplomatic, and executive information assets.

The actual legality of the proposed targets according to international humanitarian law is not discussed in this paper. Theories create models and seek to predict outcomes. It is up to the users, the policy creator, to align the actions the theory supports with other conflicting interests such as legal compliance, ethics, and humanitarian concerns.

Two model states are created as a visualization of cyber targeting in the pursuit of destabilization.

#### First - adversarial theocracy

EXAMPLE OF TARGETING MATRIX - ADVERSARIAL THEOCRACY	
Waldo's Five Factors	Example of Targets
Legitimacy	Legislature Revelation of Undisclosed Information Leaking Email and Communication Traffic from Top Echelon
Authority	Law Enforcement Information Systems Acquire of Loyalist Informers' Personal Data Inject Forbidden Material in Trusted Loyalists' Computers and Networks
Institutional Knowledge	Real-Estate/Cadastral Data Corrupting Land Ownership Information
Control	Destruction of Hard-Core Auxiliary Security Unit's Information Systems Destabilization of Financial Systems by Massive Pay-Outs of Public Funds
Confidence	Government Salary Systems Public Financial Support Transfers Real-Estate/Cadastral Data Corrupting Land Ownership Information

In a theocracy, leaders maintain societal stability and order with auxiliary police, and by utilizing government jobs as a tool to transfer funds to loyalists. The population's main asset is real-estate due to the lack of other financial opportunities, and the hidden secrets of the elite contradict their own public standards.

Life in the theocracy can be unpleasant, but it is stable, and if you are loyal to the regime you get a share of state income. The non-loyalist can maintain their wealth through real-estate ownership, which is their main private asset. By identifying this fabric through strategic cyberwar theory a swift and premeditated wave of cyberattacks could destabilize the society.

As an example, theocratic Iran with private ownership of real-estate assets, but with limited venues to gain wealth has an embedded vulnerability. Iran is well aware that it will be targeted in a cyber conflict, and has hardened military and critical infrastructure computer systems. The strategic cyberwar theory will identify the cadastral survey data as vulnerability based on the importance as institutional knowledge and confidence.

Iran's real-estate represents the bulk of privately held assets, and tampering with cadastral data will jeopardize the popular confidence in the government. A successful attack on Iranian land survey data, creating confusion regarding who owns what, and what information to trust, can create far more societal entropy and risk for regime changing violence, than attacks degrading the Iranian Revolutionary Guard information systems. The entropy from a collapse in the cadastral and land survey systems can heavily influence societal stability. If the magnitude is multiplied by other niche targets belonging to the fabric that keeps the nation calm, the theocratic regime can fall.

---

---

Cyber targeting can induce  
a sense of lack of control  
with citizens blaming the  
state for failing to safe-guard  
the societal structure.

The second example is a one party dictatorship that has successfully survived by providing consumption and financial reward to the crucial part of its citizenry. The one party dictatorship has a set of unique tenets with the government highly centralized and dictatorial. The building sector and real-estate is where money is funneled through informal banking institutions, which operate outside of the party-controlled system, with money providing mortgages.<sup>[29]</sup> The informal banking sector is an inviting target of opportunity.<sup>[30]</sup> All banks have a database that sorts out who owes what to who, while establishing demand. The database can be destroyed or corrupted with bold and swift systematic attacks of the informal banking system, which will unleash entropy. As in the theocracy, the one party dictatorship relies on pay-outs to loyalists, which then becomes a target with corrupted payments.

EXAMPLE OF TARGETING MATRIX - ADVERSARIAL ONE PARTY DICTATORSHIP	
Waldo's Five Factors	Example of Targets
Legitimacy	Deny Electricity for Iconic Administrative Centers
Authority	National Police Information Sharing Dissemination of Loyalist Informers' Personal Data
Institutional Knowledge	Real-Estate/Cadastral Data Corrupting Land Ownership Information Destruction of Permit Databases
Control	Corruption of Government Salary Pay-Outs Degrade the Blocking Operations that Prevent Access to the Complete Internet
Confidence	Informal Banking Institutions

### ***Remotely Launched Societal Destabilization***

For the attacker, the keys to successful implementation of strategic cyberwar theory is the pre-planning and mapping of the institutional design and weaknesses of the targeted society. Cyber conflict from a strategic level is a pointless exercise unless the cyber attacks influence and degrades the targeted society. The presented theory is designed to guide the development of offensive cyber operations in a strategic cyberwar between nation states.

The speed of strategic cyberwar theory negates the adaptive behavior in the targeted state. Western nations have a corporate and federal culture of rapid patch management, following the different information security management structures and protocols in place, but the potential adversarial nations have less capacity to patch their networks in time.

Rapid cyberattack ensures the feedback loop generated by the attack does not generate a system recovery. Existing patch management is too unstructured, driven by commands instead of delegated initiative, and therefore lacks rapid response mechanism.

Today, the adversarial nations' cybersecurity is managed by each agency and department independently without any over-arching strategic coordination. This absence of national coordination in these countries creates an opportunity to be exploited by strategic cyberwar theory with a systematic attack.

There are moral constraints and issues impacting the utilization of the theory to its full extent, such as the humanitarian responsibility for triggering civil war by remote control, and the contrary argument if the prolonged suffering under a ruthless regime would require humanitarian intervention, but that is a different debate.

The strategic cyberwar theory seeks to explain, put in context, and guide by providing a thought model with predictive power. This theory is not tied to today's policy; only 30 years ago, the fax machine was high tech. We cannot focus on current cyber capabilities, but instead, we need to think where cyber development is going and how it will transform societies in the future. It might be valuable to remember that the Wright Brothers first flight lasted 12 seconds and covered just 100 feet, but aviation did not wither away because the first flight was not transatlantic. In cyber, things will fall in place as new technologies emerge, which increases the need to put cyber in a strategic context.

### ***Conclusion***


The proposed strategic cyberwar theory is a work in progress, but the claims are maturing. The core assertion is that cyber will be a means to attain geopolitical goals in the future by destabilizing adversarial nations. Strategic cyberwar theory is a tool to exploit weaknesses in adversarial states. Eventually, cyber capabilities will drive adversarial countries into entropy by creating a system shock to the institutional framework holding these countries together. As stated, traditional military theory applied to cyber conflict with four challenges: anonymity, object permanence, measurable results, and rapid execution. In a Westphalian and Clausewitzian geopolitical world these challenges were non-existent. The lack of object permanence nullifies maneuver, which until now has been essential in military strategy, and it replaces object permanence with a rapidly evolving kaleidoscope of nodes and bits. The massive anonymity in digital interchanges removes the ability to clearly understand who is your enemy, and based on that assessment gauge their abilities. Finally, with no measurement of effectiveness a fighting nation is unaware of the actual impact of the interchanges in tactical time frames and the rapid execution is likely to create a battle of which only the machines are fully aware. These four unique cyber tenets evaporate the opportunity to use traditional military thinking in cyber. If traditional military thinking is utilized to formulate a strategy, it is likely that the result would aggregate spurious assumptions and remove the opportunity for decisive offensive cyber operations as a geopolitical toolset.

---

---

Strategic cyberwar  
theory predicts the  
weaknesses of targeted  
governments, and  
assists in remotely  
initiated regime shift  
or submission to  
foreign power.

Strategic cyberwar theory views the adversarial nation as a framework of institutional arrangements instead of a set of military assets and digital networks. The institutional frameworks are likely to be less well defended as the industrial-military complex, but when destabilized these frameworks remove the underpinnings of the adversarial regime leading to a decisive climax to the cyber conflict. The theory also argues that attacks have to occur within a limited time frame to ensure system shock in the targeted society.

Strategic cyberwar theory addresses the unique tenets of the cyber domain: anonymity, object permanence, measurable results, and rapid execution. The theory avoids the need to identify the enemy, rely on maneuvering and object permanence, require measurable tactical results, and be independent of need for actionable leadership under conflict. The strategic cyberwar theory provides a way to create a decisive strategy for nation state conflicts. 

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*

## NOTES

1. Paul Brooker, *Non-Democratic Regimes: Theory, Government and Politics* (New York: Palgrave Macmillan 1994).
2. Bruce, Russett, and Maoz Zeev, 'Normative and Structural Causes of Democratic Peace', *American Political Science Review* 87 3 (1993), 624-638.
3. Bruce Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press 1993).
4. Thomas Rid, *Cyber War Will Not Take Place*, (Oxford: Oxford University Press 2013).
5. Jan Kallberg and Bhavani Thuraisingham, 'Cyber Operations: Bridging from Concept to Cyber Superiority', *Joint Forces Quarterly* 68 (2013).
6. Applegate, Scott D, 'The Principle of Maneuver in Cyber Operations', In *Cyber Conflict (CYCON)*, 2012 4th International Conference on, 1-13. IEEE, 2012.
7. Jan Kallberg, Bhavani Thuraisingham, and Erik Lakomaa, 2013, 'Societal Cyberwar Theory Applied the Disruptive Power of State Actor Aggression for Public Sector Information Security', Presented at and published in *Proceedings from the 2013 IEEE European Intelligence and Security Informatics Conference (EISIC 2013)*.
8. John Shand, *Philosophy and Philosophers: An Introduction to Western Philosophy*, (Montreal: McGill-Queen's Press-MQUP 2002).
9. Jan Kallberg, and Adam B. Lowther, 'The return of Dr. Strangelove', *The Diplomat*, August 20, 2012.
10. William H. Webster, Frank J. Cilluffo, and S. Lanz, *Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: Center for Strategic & International Studies 1998).
11. Ariana Eunjung Cha, 'For Clarke, a Career of Expecting the Worst: Newly Appointed Cyberspace Security Czar Aims to Prevent Digital Pearl Harbor', *Washington Post*, Nov. 4, 2001.
12. Alison Mitchell, 'To Forestall a 'Digital Pearl Harbor,' U.S. Looks to System Separate From Internet', *New York Times*, November 17, 2001, <<http://www.nytimes.com/2001/11/17/technology/17INTE.html>>
13. Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35 1 (2012), 5-32.
14. Hans Wilhelm Gatzke, ed, Carl von Clausewitz: *Principles of War*, (New York: Military service publishing company 1942).
15. Jan Kallberg, and Bhavani Thuraisingham, 'Cyber Terrorism to State Actors' Covert Cyber Operations in *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies*', Babak Akhgar and Simeon Yates, eds. (Oxford: Butterworth-Heinemann 2013).
16. Paul Pierson, 'Increasing Returns, Path Dependence, and the Study of Politics', *American Political Science Review* (2000), 251-267.
17. Paul Pierson, *Politics in time: History, institutions, and social analysis*, (Princeton: Princeton University Press 2004).
18. Heinz Guderian, *Panzer Leader* (New York: Dutton 1952).
19. Kenneth N. Waltz, 'Nuclear Myths and Political Realities', *American Political Science Review*. -- (September 1990), 731-745.
20. Schmitt, Michael N. ed, *Tallinn manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University Press 2013).
21. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle: U.S. Army War College – Strategic Studies Institute 2013).
22. Martin C. Libicki, 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly*, (2014, Spring).
23. Libicki, 'Why cyber war will not and should not have its grand strategist', 29.



## NOTES

24. Jan Kallberg, and Rosemary A. Burk, 'Cyber defense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations' in *Conflict and Cooperation in Cyberspace - The Challenge to National Security in Cyberspace*. P. A. Yannakogeorgos and A. B. Lowther, Eds, (New York: Taylor & Francis 2013).
25. Jan Kallberg, and Rosemary A. Burk, 'Failed cyberdefense: The Environmental Consequences of Hostile Acts, *Military Review*. (May-Jun. 2014), 22-25.
26. Dwight Waldo, *The Administrative State*, (New York: Holmes & Meier Publishers 1948).
27. Dwight Waldo, *The Enterprise of Public Administration* (Novato: Chandler & Sharp 1980).
28. Jürgen Habermas, *Legitimation Crisis* (Boston: Beacon Press 1975).
29. Kellee S. Tsai, *Back-alley banking: Private entrepreneurs in China* (Ithaca: Cornell University Press 2004).
30. The Economist, 'Shadow banking in China - The Wenzhou experiment', April 7, 2012, <http://www.economist.com/node/21552228>>.

# Is There a Cybersecurity Dilemma?<sup>1</sup>

---

Dr. Martin C. Libicki

A security dilemma is said to exist when one country cannot make itself more secure without making another less secure.<sup>[2]</sup> Circa 1913, for instance, if a major European country sought security by drafting more men, its neighbors would feel impelled to do likewise to recover their former levels of security. During the Cold War, when deterrence was the only feasible response to threat posed by the other side's nuclear weapons, any attempt to build more weapons or bring them to a higher state of readiness (for retaliatory purposes only, it would be claimed) would alarm the other side who would feel impelled to do likewise.

Is the same true in cyberspace? Might one country's attempt to increase its cybersecurity come at the expense of the cybersecurity *perceived* by potential adversaries?

In answering this question, two qualifications merit consideration. *First*, cybersecurity—efforts to prevent systems from being compromised—is useful against multiple threats. Some threats are purely criminal. Others are espionage, often but not always state-sponsored. Yet others are potentially disruptive or destructive, again often but not always state-sponsored. Although, it is possible to make a fair guess regarding the cost of cybercrime, the cost of espionage is conjectural (much depends on how purloined information is later used), and the losses from disruptive or destructive effects relatively low in much the same way that the costs associated with the destruction from nuclear war is currently zero. But the latter cannot be ignored, inasmuch as security is measured in terms of a contingent future, which may very well feature destructive cyberattacks among countries at war. *Second*, one must distinguish between whether one country's cybersecurity will, *in and of itself*, increase or decrease another country's cybersecurity, and whether a *particular action* to increase one country's cybersecurity will increase or decrease another country's cybersecurity. For instance, one country's



Martin Libicki (Ph.D., U.C. Berkeley 1978) has been a Distinguished Visiting Professor at the U.S. Naval Academy and a Senior Management Scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. In addition he is a Distinguished Visiting Professor at the U.S. Naval Academy and has been an adjunct at Columbia University and Georgetown University. He wrote two commercially published books, *Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte* and has a textbook (*Cyberspace in War and Peace*) at the publisher's (U.S. Naval Institute Press). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, and *Crisis and Escalation in Cyberspace*. Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

eliminating its own botnets will increase its own and everyone else's cybersecurity. However, one country's adopting particular active defense measures (such as intervening in another country's network to look for malware about to be deployed) may increase its own cybersecurity and decrease others'.

We now address the question in two parts: economics and international relations.

### *An Economics Perspective*

When discussing whether one party's activities make another worse off, economists like to talk about externalities. They can be negative or positive. A negative externality, for instance, is created when my neighbor's smoke gets into my lungs. A positive externality is created when my neighbor's well-tended garden improves the view from my kitchen window. Correspondingly, if my cybersecurity activities make your networks less secure, then I am creating negative externalities; such activities should be discouraged (e.g., by taxing them) accordingly. If, conversely, my activities make you more secure, then I am creating positive externalities and they should be encouraged (e.g., by subsidizing them).

Positive externalities from improving cybersecurity are many and various.

One of the more oft-cited examples deals with bots. If I fail to keep my computer up to date with security patches, or if I practice less-than-perfectly-safe web surfing or e-mail practices, then my personal computer could be compromised. Many, perhaps most, of these compromised computers will become a bot, that is, a machine capable of being commanded to spam this or that site. Typically, thousands or millions of such bots are shepherded into botnets. Botnets, in turn, can be used to mount distributed

denial of service (DDOS) attacks to stifle access to parts of the Internet. Motives for DDOS attacks range from personal and political (Iranian attacks on US banks<sup>[3]</sup>) to criminal (pay us or we will shut down your gambling site just when wagers are being made). Many regard the DDOS potential arising from home users failing to maintain their machine's cybersecurity as so serious that they advocate allowing, or even mandating, Internet Service Providers to shut access to customers whose machines have been turned into bots.<sup>[4]</sup> It is unclear how such a policy might work in the coming future when most such machines are Internet-connected devices (e.g., thermostats, children's toys) whose owners are unaware that they are even networked.

A more direct version of herd immunity arises in the way viruses and worms can spread from one machine to another. The cleaner my machine is, the more likely it can ward off infection, and hence, less likely that it will infect you. The Internet was convulsed with a series of rapidly-spreading worms, starting with Code Red in 2001, and continuing on through NIMDA, MSBlast, SoBig, MyDoom, Slammer, and Witty among others. But a patch to Microsoft XP (Service Pack 2) released in August, 2004 essentially eliminated that particular threat. Although replicating malware exists—indeed, hackers rely on malware with such properties to move laterally within an organization—its spread is generally limited to machines that use common services (e.g., printers, file shares), and, hence, rarely leaves the confines of organizations. They do not spread globally within hours as the earlier versions did.

There are also general forces that promote herd immunity in cyberspace. The greater the percentage of ill-secured machines connected to the Internet, the greater the potential rewards for cyber-criminals. Not only is there a larger target set, but the odds of turning a random machine are higher; both offer more reward per unit of effort. The greater the rewards for criminality, the greater the investment that criminals will make in improving their capabilities. The same logic works for providers of cybersecurity services. The more diligently users—notably, organizations with complex networks—attend to cybersecurity the larger the market they create for such providers (\$75 billion a year in sales and growing<sup>[5]</sup>), and the greater the incentive for start-ups (of which there are thousands) to invent better mouse-traps. Again, my greater diligence means more and better products for you to use. Even if individuals rarely buy such merchandise themselves, they show up in products people use, such as web browsers. Finally, the more secure an infrastructure is, particularly against data theft, the more people can engage in electronic commerce without undue worry—and that also benefits all.

---

A security dilemma is  
said to exist when one  
country cannot make  
itself more secure  
without making  
another less secure.

Conversely, those who remember the joke that ends, “I don’t have to outrun the bear, I just have to outrun you,” might counter that if it is too easy for criminals to prey on certain users, they may not have to improve their arts to make money. Thus, they would leave the more fastidious users alone, and turn their attention to the less fastidious. If so, one person’s sloppiness gives them an easy target, and increases the odds that they can satisfy themselves without working hard to attack another person. The difficulty in predicting as much beforehand arises from trying to understand what role signaling plays in the relationship between one person’s cybersecurity and another’s. Hackers may have little *a priori* knowledge of who is or is not an easy target. In 2015, a spokesman for a cybersecurity startup made the claim that an APT attack was not only thwarted, but discouraged from continuing to batter an organization that had purchased one of the startup’s products after the product was discovered working on a target server.<sup>[6]</sup> Consider piracy as an analog. The more treasure ships that roam the high seas, the more opportunities for pirates, the greater the incentive to become one. Conversely, the more treasure ships that roam the seas, the less likely the existing crews of pirates will pick on mine. Now assume that some of these treasure ships are armed enough to imperil pirate ships. Once this is so, piracy carries grave risks. If pirates cannot determine which ships are armed

---

The greater the percentage of ill-secured machines connected to the Internet, the greater the potential rewards for cyber-criminals.

before confronting one, then they will hesitate to attack any ship. The benefits from some being armed accrue to all ships. However, armed ships might want to advertise that fact because it helps them avoid confrontations in the first place, which is preferable (unless they have been armed by, say, a government for the express purpose of eradicating the pirate menace) to enduring the damage and casualties of winning a confrontation. Unless unarmed ships can appear to be armed, they are scarcely better off for there being armed ships. In that case, there are no positive externalities.

The closest analogy to ship signaling here may be information sharing, which is an unquestionably good thing (irrespective of the merits of any one piece of legislation to foster information sharing). Two forms of information sharing merit note: general and specific. General benefits occur when organizations share among themselves stories of how their own failures and bad choices allowed them to be hacked. As in aeronautical engineering or medicine, knowledge (and safety) advances one bad outcome at a time—as long as these outcomes are shared and dissected for lessons learned. The more people who share, the more examples are shared, and the faster the knowledge base grows (even as hackers, themselves, share information), and thus the greater the skill base for repelling hackers. Specific benefits occur when organizations share information about specific

hackers (e.g., Unit 61398 identified by the Mandiant Corporation<sup>[7]</sup>) who have a particular repertoire of malware, social engineering tricks, or the like. Such knowledge allows organizations, notably those with sophisticated firewalls or intrusion detection systems, to use the signatures generated by this information to block intrusions. Conceivably, telltale signs of compromise may be shared to detect and eradicate infections that have already taken root in an organization's networks. If the global cyber community gets to the point where such information can be routinely shared, the odds of a sufficiently broad attack (where the same indicators can be found over large numbers of different organizations) can become vanishingly small even if individual system compromises can remain undiscovered for long periods of time (these days, the average APT attack goes unnoticed for an average of seven months<sup>[8]</sup>).

There is a broader lesson here about incentives and institutions. The neoclassical market beloved by economists is built around a model of large numbers of small decision-makers whose decisions might produce externalities. Incentives are manipulated so that positive externalities are encouraged and negatives ones discouraged. But the world of cybersecurity is one of institutions. Rapidly replicating worms did not stop because users were penalized for being sloppy, but because one organization (Microsoft) altered its product to disable such worms. Information sharing will only begin to benefit cybersecurity after institutions arise that find systematic ways of converting information into knowledge and practice.

### ***An International Relations Perspective***

The problem, viewed from an international relations perspective, assumes an anarchic world in which countries do, in fact, threaten one another in cyberspace. Such threats could be used to support conventional kinetic capabilities: e.g., if I can disable your anti-aircraft weapons, my threat to bomb you would have greater credibility. They can also be used independently of armed conflict: if you intervene in my back yard, I will create chaos in your banking system.

To address whether one nation can increase its cybersecurity without another nation's cybersecurity being reduced requires some context. For many forms of combat, the same weapon can be used for offensive and defensive purposes. If a country fears a million infantry on its border (*circa* WWI) its most basic military response is to raise a million infantry on its own borders; it could announce that its infantry's purpose was defensive,

---

The more secure an  
infrastructure is,  
particularly against data  
theft, the more people  
can engage in electronic  
commerce without  
undue worry—and that  
also benefits all.

but no one could assume that such forces could not go on the offense. With nuclear weapons in the Cold War, nothing was defensive. The doctrine of deterrence would not have been so compelling had satisfactory defenses been available.

But while the security dilemma is harder to avoid if all defensive weapons were, at the same time, potentially offensive, the dilemma does not disappear if there were truly defensive weapons. *Circa* WWI, forts on the Western Front were defensive weapons; after all, they sat in a country's own territory. But the other side could argue that nothing was as offensive as a good defense because it permitted one side to attack with reduced risk. Their forts would limit the risk of failure by allowing a much smaller force to stay back and defend the territory against unexpected reverses or occasional enemy break-outs. Although US (conventionally-armed) anti-ballistic missiles (ABMs) were totally defensive, they frightened the Soviet strategists who believed the United States, so protected, could launch a first strike without fear of repercussions. Cybersecurity works the same way; *most* of what brings about cybersecurity (e.g., better computer hygiene) cannot possibly make others less secure *directly*—but could conceivably make others less secure *indirectly* by encouraging cyberattacks by those who convince themselves that their own cybersecurity makes them invulnerable to retaliation.

Central to this logic was that when discussing WWI ground forces, or Cold War era nuclear weapons, countries were at the top of their escalation ladder. It is not as if someone could trump these force elements with other unused weapons at their disposal. Cyberattacks, of course, can be trumped—certainly by nuclear weapons, and almost as certainly by strategic bombing and conventional land operations. It is difficult to imagine that the costs of a strategic cyberattack campaign would exceed that of even a small war, particularly if cost and coercion are measured in terms of human casualties; after all, no one has died yet as a direct result of a cyberattack. Thus, the degree of insecurity in one country that may arise from the fact that their enemy's society enjoys cybersecurity is limited to the pain that it is willing to take without escalating to physical force. This pain is not zero because there are good reasons not to let a fight in cyberspace bleed over into the physical world—but it *is* limited.

But does that mean that greater cybersecurity in one country will always reduce the security of another? Not directly, in most cases. To begin with, almost all defensive actions in cyberspace are unmistakably defensive: examples include measures such as diligent patch management and least privilege, multi-factor authentication, and intrusion detection systems. They cannot be used to break into systems, in large part, because such actions take place within the computer networks being defended (aka *blue space*).

But there are exceptions, many of which fall under the rubric of active defense. If President Obama's speech defending his management of the NSA is any indication, offensive capabilities are a vital part of cybersecurity defense.<sup>[9]</sup> It is easy to imagine how poking around in the attacker's networks—*red space*—might provide indications and



warning of a cyberattack, just as it might reveal indications and warnings of plans to use physical force. Private organizations routinely crack servers, many of them belonging to third parties—*gray space*—looking for evidence that their own stolen files are sitting there; in doing so they collect information that allows the tracks of attackers to be found in the systems they are defending. Other defenses have been known to disable the computers from which attacks are coming from (one from the late 1990s caused the attacker’s computer to keep throwing up new windows onto the screen). There was even a case in which the defender left a corrupted file out for the attacker to grab and open, which then infected the attacker’s machine, and took a screen shot of the perpetrator.<sup>[10]</sup> These are instances where the ability to defend relies on the ability to attack—and, in many cases, the victims of such attacks are not only systems owned by the original attacker, but any system in the attacking country.

But how much concern should be associated with these techniques before concluding that what brings me cybersecurity brings you cyberinsecurity? Most of these offensive defenses can be warded off by attackers who anticipate that they themselves may be attacked. For instance, when electronic intelligence collection is a problem, isolation provides much of the solution (for those operations that require access to the outside world, hackers could, for instance, use a computer and an IP address once, and then move on). When there are prospects that code in one’s repositories could get altered before being delivered, digital signatures can assure authenticity. Obfuscation and encryption techniques can inhibit what others can collect from intermediate servers in gray space. And all the techniques that rely on returning poisoned materials to the attacker can either be filtered out (e.g., by accepting only pre-selected inputs) or can be transferred to an isolated computer for the latter to process (*that* computer may be infected but it cannot be controlled by the target because of its isolation). These techniques are not free, and some (such as filtering) require some sophistication, but if cyberwar is serious, then these active defense techniques are hardly speed bumps, much less barriers.

If there is a clean separation between defensive and offensive techniques, then the cybersecurity dilemma therefore has to be indirect: my improved cybersecurity emboldens me to attack your systems. The major impediment to this formulation is whether confidence in one’s own security is merited. Alternatively, my cybersecurity will reduce your confidence in prevailing in a confrontation, and therefore you will yield even at the expense of your *broad*er security goals; here the issue is the other side’s confidence in *your* cybersecurity.

---

---

Information sharing  
will only begin to benefit cybersecurity after institutions arise that find systematic ways of converting information into knowledge and practice.



But can aggressors legitimately feel that their systems are impenetrable or even sufficiently well protected to the point where they can convince themselves that their losses from cyberattack are manageable regardless of what their foes might do? Consider the first clause. North Korea may be impenetrable (although even they are becoming gradually more connected), but only because North Korea has crippled its own economy in the service of *juche* (roughly: self-reliance). Yet most normal countries are increasingly dependent on information systems and growing more so by the day. As a general rule, any Internet-exposed system built on personal computers cannot be protected reliably against an even-halfway sophisticated opponent absent enormous expenditures on cybersecurity.<sup>[11]</sup> Only a fool can be confident that having traced out all possible attack vectors and having figured out how to block them, conclude that it was perfectly secure. Not only are systems become far too complicated to know all possible attack vectors, but there is very little software that lacks (zero-day) vulnerabilities. And this does not include other sources of non-technical vulnerabilities such as suborned insiders or sloppy users. True, our computers are far more vulnerable than they need to be—Apple’s iOS operating system, because of its closed nature is two orders of magnitude safer than PC operating systems (even though MacOS is no more secure than Microsoft Windows). And machines whose every instruction is burned into hardware cannot host malware once they have been turned off and back on. Nevertheless, even a world without malware is not a perfectly secure world because complex software is heir to unwanted results (e.g., a deliberately malformed database query can often persuade databases to spill their contents unexpectedly), and because authentication and authorization is still an art not a science.

If it is hard for an aggressor to feel deservedly confident in its invulnerability to counter-attack, the other side might not necessarily feel as if its own efforts to penetrate adversary systems are futile. This works both ways. The aggressor may know what investments it has made to ensure its cybersecurity, but if the other side is testing the aggressor’s defenses by trying to compromise its systems, it may know more than the aggressor about how far it was able to get. What attackers may not know is what the effects of its cyberattack successes might be on its target’s ability to get work done (for instance, the target may have secret back-up capabilities), or its ability to recover quickly from having been attacked.

In practice, rational aggressors are going to look at a vast tableau of capabilities, both offensive and defensive, when making threats or carrying them out. The more confidence they have in their cybersecurity the bolder they are likely to be, but there are so many assumptions packed into the cybersecurity relationship; enhancing actions, actual cybersecurity and perceived cybersecurity on the one hand, and the relationship of cybersecurity to overall *defensive* capabilities *plus* the relationship of defensive capabilities to the ability to take to the offense, that the gearing between investing in cybersecurity, and posing a threat to neighbors may be vanishingly small. It is worth remembering that cybersecurity has uses beyond simply warding off attacks from

enemy countries: other reasons include attacks from insiders, spies from every imaginable country, whoever is calling themselves *Anonymous* this week, and even the run of disasters, accidents, and bad software (improving resilience, for instance, preserves a system's capabilities against threats from human error, acts of nature, and bad software).

Another facet of cybersecurity which dulls the security dilemma is the difficulty one side has in knowing what the other side is doing to secure its networks. In 1914, when one country mobilized, its foes were persuaded to do likewise for fear of falling behind in the coming conflict, and despite some desultory attempts (largely, by Russia) to hide the fact of mobilization, few were fooled. In the nuclear context, putting forces on alert in response to a crisis exacerbated a crisis in the mind of the other, since the only logical response to a nuclear threat in a world of deterrence was to increase the threat that one could reciprocate to an adversary.

One of the factors favoring stability in cyberspace—counterintuitively for a medium in which everything supposedly works at the speed of light—is that it is difficult to detect quickly when the other side is advancing its capabilities. Cyberwar is usually an activity whose tools are deeply hidden (because if one knew how attack tools worked, defeating them would be a straightforward matter of fixing or routing around the vulnerabilities they exploited). If one goes by what attackers have actually done, there is a lag (measured in weeks and months) between the decision to attack a target, and its successful penetration and then (notably for espionage and subtle corruption) there can be an additional lag between the action and its detection. It can also be difficult to react *defensively* to the other side's quick improvements. Even if patches can be installed, literally, within minutes, the more fundamental changes in computer code and network architecture (e.g., restricting access privileges, adjusting input filters) take time to create and test. On the offensive side, the key to increased capability is not more weapons (it is trivially easy to replicate malware), but better weapons, notably those that work against hitherto, undetected vulnerabilities. The latter can take time, often an unpredictable time, to develop.

The cybersecurity dilemma fades further when countries start depending on the same infrastructure for their cybersecurity. In one sense they already do: commercial software is a global commodity, and cybersecurity firms take customers from anywhere. Vulnerabilities for one are vulnerabilities for all; patches for one are patches for all. If and as cloud computing spreads, various countries may find themselves dependent on the security of the same providers. It will be interesting to see how moves towards autarky in cyberspace

---

---

Rational aggressors are going to look at a vast tableau of capabilities, both offensive and defensive, when making threats or carrying them out.

(notably by Russia, itself following the lead of Iran and North Korea) affect such trends.

Finally, cybersecurity is useful against both espionage and attack. Increasing cybersecurity in one country may make it difficult for another country to collect intelligence on it (or not: it may take an unaffordable level of cybersecurity to keep a really professional espionage agency from collecting most of what it needs from Internet-connected networks). The failure to collect intelligence may lead to insecurity; note how vociferously the FBI and NSA criticize the access to hard-to-break encryption technologies that they claim terrorists now enjoy.

### ***The Calculus of Insecurity***

Ultimately, any security dilemma is about the relationship between two countries. If both live in a zero-sum world in which it is not stability and security that both sides seek, but power vis-à-vis the other, then, everything touches the security dilemma because nothing will make both sides more powerful *vis-à-vis* the other. But this condition is rare. Even dedicated mutual enemies such as ISIL and the United States can have common objectives (e.g., changing the Syrian regime; limiting Iranian influence).

More commonly, every country has a mixed relationship with every other country. Russia and the United States may view each other with suspicion regarding former Soviet countries (e.g., Ukraine), but both of them have criminals as common enemies. Cybersecurity that protects systems from being compromised by criminals is largely the same cybersecurity that protects systems from being compromised by anyone else, notably other countries. If a country improves its cybersecurity by catching criminals, there will be fewer criminals; thus the other country is better off. If countries care about preventing crime more than they worry about each other, they share a mutual interest in improving cybersecurity.

Last, it helps to remember that security is not just the feeling that one can withstand an adversary's attacks, but also the feeling that an adversary is unlikely to try. This introduces a paradox that affects all forms of warfare: countries may be motivated to start trouble not only because they are fearless but fearful (and believe that it must act before falling irretrievably behind). Similarly, they may overreact to events because they are twitchy and believe that the failure to act will leave them exposed to surprise attack. Both factors were in play to start WWI. Germany was concerned with a rising Russia, and all sides feared being out-mobilized by potential foes.

In cyberspace, ambiguity can make such fears take a malign form. It is difficult to tell who is attacking whom in cyberspace (and for some attacks, it is often difficult to know, even afterwards, what information was taken or what processes were corrupted). Distinguishing cyber-espionage from an impending cyberattack when a hostile implant (inserted back door) is found is difficult because one implant can be used to do both.

Cyberwarriors may believe (notwithstanding the lack of corroborating facts) that they can pre-empt planned cyberattacks by carrying out cyberattacks on potential attackers. In the fog of misperception, a nervous country may be apt to assume the worst and lash out to protect itself; by so doing it may start a fight that a more secure country might have avoided.

In the end, the major policy question is whether to enable or disable cyberwar for everyone by promoting a global culture of cybersecurity and waging incessant war on vulnerabilities and ignorance. Those who think that the United States is currently in a no-holds-barred contest with other major powers may think such efforts naïve. Others who think that cyberwar provides a chance for countries to contest without serious consequences—when alternative forms of contestation may kill people—may think such efforts counterproductive. But those who think that creating new forms of conflict generally detracts from everyone’s ability to get along may want to give the matter serious thought. In the end, there is less of a cybersecurity dilemma than it seems. 🛡️

## NOTES

1. See for instance, Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics*, 30, 2, (January 1978), 167-214.
2. Nicole Perloth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013; <http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html>.
3. Something similar has been used in Australia; see Sean Gallagher, "Is an ISP code of conduct the best way to fight botnets?," *Ars Technica*, September 22, 2011, <http://arstechnica.com/business/2011/09/us-government-looks-to-fight-botnets-with-isp-code-of-conduct/>.
4. "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach \$75.4 Billion in 2015," September 23, 2015; <http://www.gartner.com/newsroom/id/3135617>.
5. Andrea Shalal, "U.S. firm CrowdStrike claims success in deterring Chinese hackers," *Web Culture*, April 14, 2015, [http://www.webculture.com/17/Tech%20Top%20News/16/a/19280884/US\\_firm\\_CrowdStrike\\_claims\\_success\\_in\\_deterring\\_Chinese\\_hackers](http://www.webculture.com/17/Tech%20Top%20News/16/a/19280884/US_firm_CrowdStrike_claims_success_in_deterring_Chinese_hackers).
6. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (report, 2013), [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).
7. Statement for the Record by Richard Bejtlich Chief Security Strategist FireEye, Inc. Before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations Understanding the Cyber Threat and Implications for the 21st Century Economy, March 3, 2015; <http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-Wstate-BejtlichR-20150303.pdf>.
8. We cannot prevent ... cyberthreats without some capability to penetrate digital communications, whether it's to ... intercept malware that targets a stock exchange, to make sure air traffic control systems are not compromised or to ensure that hackers do not empty your bank accounts. From "Transcript of President Obama's Jan. 17 speech on NSA reforms," *Washington Post*, January 17, 2014, [http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcd84\\_story.html](http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcd84_story.html).
9. Charlies Osborne, "Georgia turns the tables on Russian hacker," *ZDNet*, October 30, 2012, <http://www.zdnet.com/georgia-turns-the-tables-on-russian-hacker-7000006611/>. The target planted malware in a file that the hacker took. The hacker's computer was infected when the file was opened. The computer's webcam then turned on and photographed the presumed hacker.
10. Circa 2014, JPMorgan Chase's annual expenditures of \$250 million a year did not prevent their systems from being hacked (although they may have prevented the hack from having consequences more serious than the release of information normally found in phone books); see Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perloth, "JPMorgan Chase Hacking Affects 76 Million Households," October 2, 2014; <http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>.

# Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies

---

Francesca Spidalieri  
Jennifer McArdle

Information communication technologies (ICTs) have become the foundation—both the bone marrow and connective tissue—of modern militaries. Satellites, precision guided munitions, nuclear launch systems, helicopters, and any number of other weapon platforms are reliant on ICTs for their operational capability and connectivity. No modern military can enter the battlespace without some reliance on cyberspace for their land, sea, air, space, or information operations. Moreover, the ‘battlespace’ is no longer reserved solely for ‘war time’. Cyberspace has blurred the lines between traditional conflict and peace, and states are finding themselves in a position of protracted, low-level conflict in the cyber realm. While this conflict often takes the form of cyber crime, cyber espionage or service disruption, the specter of a large-scale armed conflict conducted wholly or partially in cyberspace, continues to rise.<sup>[1]</sup> And while cybersecurity is not solely a defense challenge, the US military’s increasing reliance on cyberspace, alongside the growing array of cyber threats and vulnerabilities, has made securing this space and establishing a competitive advantage on the modern battlefield a leading priority for any military in the 21st century.

In response to the proliferation of cyber threats, the White House raised the US Department of Defense (DoD) FY2016 cyber budget to \$9.5 billion, an 11 percent increase in spending over FY2015.<sup>[2]</sup> The recently published DoD Cyber Strategy seeks to strengthen the US’ cyber defense and deterrence posture by building cyber capabilities and organizations around three critical cyber missions: the defense of DoD networks, systems, and information; the defense of the US and its interests against cyber attacks of significant consequence; and the provision of cyber capabilities to support military operations and contingency plans. Despite a stated emphasis on defense and deterrence, the document also highlights the wide arsenal of DoD’s offensive cyber capabilities that could be employed in the event of a conflict.<sup>[3]</sup>



Francesca Spidaliere is the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University, where she leads the Cyber Leadership Research Project and the Rhode Island Corporate Cybersecurity Initiative (RICCI). Francesca has been appointed by Governor Gina Raimondo to the Rhode Island Cybersecurity Commission, and serves also as subject-matter expert for the Potomac Institute for Policy Studies' Cyber Readiness Index Project, the Center for Internet Security's Roles & Controls Panel, and the Ponemon Institute. Her academic research and publications have focused on cyber leadership development, cyber risk management, cyber education and awareness, cybersecurity workforce development, and the professionalization of the cybersecurity industry.

She holds a B.A. in Political Science and International Relations from the University of Milan, Italy; and an M.A. in International Affairs and Security Studies from the Fletcher School at Tufts University.

Strategy and funding alone, however, are not sufficient to achieve a fully capable military force. The military must also have highly-trained, cyber-capable personnel and leadership prepared to meet tomorrow's challenges today.<sup>[4]</sup> As Representative Jim Langevin stated:

The greatest challenge faced by the Department of Defense—and the entire government enterprise—is human resources. Technological dominance is meaningless without a skilled workforce capable of operating at the highest level of their field. In this area, we are falling short.<sup>[5]</sup>

This article addresses the role that US service academies play in developing not only future cyber forces, but also a pipeline of qualified cyber-strategic military leaders, who have the knowledge necessary to confront a wide array of cyber threats and establish both a competitive and security advantage in the modern battlespace. In the future, *every military leader must be a cyber-strategic leader*. In particular, this study surveys current efforts by the US Coast Guard Academy, the US Air Force Academy, the US Military Academy, and the US Naval Academy to prepare all their future officers for the challenges of operational- and strategic-level leadership in an age of persistent cyber threat.<sup>[6]</sup> This survey provides an overview of the level of exposure to cyber issues that cadets and midshipmen receive during their undergraduate studies at the service academies, and to what extent they graduate with an adequate understanding of the cyber challenges facing their respective services. Lastly, this article identifies some of the gaps in the existing curricula and offers preliminary recommendations to include a stronger cybersecurity component into current programs.





Jennifer McArdle is a Fellow in the Center for Revolutionary Scientific Thought at the Potomac Institute for Policy Studies. She leads a program on simulation and virtual reality for next generation warfare and also serves as a subject matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index Project. Her academic research focuses on potentialities for inadvertent escalation from "cyber warfare," national security, and military innovation. Her work has featured in outlets such as Real Clear World, The National Interest, National Defense Magazine, GovInfoSecurity, among others.

Ms. McArdle is a Ph.D. candidate in War Studies at King's College London. She holds a M.Phil in Politics from the University of Cambridge and a B.A. in Political Science and Justice Studies, summa cum laude, from the University of New Hampshire.

### ***The Next Generation of Military Leaders Must Also Be Cyber-Strategic Leaders***

The growing scope, pace, volume, and sophistication of cyber threats, and the development of cyber tools as technical weapons have been accompanied by another realization: there are few people, whether civilian or military, equipped with knowledge sufficient to protect the nation's critical infrastructure and sensitive information, improve resiliency, and leverage information technology for strategic advantage.<sup>[7]</sup> As a result, government efforts to provide cyber training for civilian and military personnel, and to create a specialized cyber workforce have become increasingly important to national security.<sup>[8]</sup>

Indeed, out of the FY2016 DoD cyber budget, \$500 million have been specifically allocated for the implementation and support of Cyber Mission Forces (CMF) tasked with training and supporting cyber personnel, both civilian and military.<sup>[9]</sup> CMF, unveiled in 2013, plans to add approximately 6,000 people split between three cyber forces, each with specific missions: defense of the nation from foreign adversaries; cyber support of the combatant commands; and protection of military networks and, when authorized, other infrastructure.<sup>[10]</sup> Thus, DoD's main efforts in this area have been largely focused on training cyber warriors, those highly specialized individuals with extensive technical training who can engage in the defensive and offensive cyber operations critical to mission effectiveness.<sup>[11]</sup> As Secretary of Defense Ash Carter noted during a recent speech in Silicon Valley, the CMF are far more valuable than the technology they use, and the DoD's "first strategic goal is building [these] Cyber Mission Forces."<sup>[12]</sup>



Compounding the shortage of highly trained cyber forces, are the increasing scale, complexity, and continuous growth of DoD networks that are providing new avenues for adversary exploitation. In 2011, the DoD cyberspace architecture was already the largest in the world, including over 15,000 networks and seven million computing devices spread across hundreds of installations globally.<sup>[13]</sup> Today, the networks continue to expand adding new features and assimilating new technologies, such as mobile devices and cloud computing.<sup>[14]</sup> Moreover, the weapons platforms that are critical to national security and deterrence: nuclear weapons, cruise and ballistic missiles, helicopters, fighter aircraft, and any number of other systems including precision guided weapons are dependent on the reliance and functionality of microelectronics, or chips, which make up the cyber hardware of the system.<sup>[15]</sup> Thus, every member of the US military regardless of whether they are in the infantry, surface warfare, logistics, maintenance, or even the chaplaincy will need some degree of cyber know-how. ICTs are already intrinsically linked to most

---

This article identifies some of the gaps in existing service academy curricula and offers preliminary recommendations to include a stronger cyber-security component into current programs.

components of military careers and missions. As the Deputy Director of the Army Cyber Institute, Dr. Fernando Maymí, stated “it will be impossible for any future leader not to acknowledge cyber issues in their decision-making process.”<sup>[16]</sup> Therefore, it is increasingly important that all military leaders, regardless of their specialty, have the requisite knowledge, technical acumen, and strategic vision to lead their Soldiers, Sailors, Airmen, and Marines into a battle-

space that is increasingly dominated by technology.

Yet, while DoD’s efforts to create a capable cyber workforce are commendable, we cannot expect the new cyber forces to be the only ones in charge of preventing, mitigating, and containing cyber threats, nor will advanced technology alone be sufficient to protect all of DoD’s networks and digital assets. There needs to be a concerted effort to develop a new generation of cyber-strategic leaders who will lead, manage, and oversee cyber defense and cyber operations in this dynamic and ever-changing digital environment. These individuals do not necessarily need specific training in engineering or programming, but they must have a deep understanding of the cyber context in which they operate, complimented by an appreciation of military ethics, strategic studies, political theory, organizational theory, history, international law, international relations, and additional sciences.<sup>[17]</sup> Indeed, future cyber-strategic leaders should extend beyond so-called “cyber warriors.” Every future military leader must be a cyber-strategic leader.

### *The Role of the Service Academies in Preparing Leaders for an Age of Persistent Cyber Threat*

The first step in the creation of both cyber warriors and a new cadre of cyber-strategic leaders is education, both at the undergraduate and graduate level. However, as the National Research Council has observed, “cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.”<sup>[18]</sup> Universities, colleges, and in this case service academies, are best fit to serve as incubators of cyber-strategic leaders, “bringing together theory and doctrine, with methodology, tools, and implementation.”<sup>[19]</sup> Cyber-strategic leadership, in fact, is not the same as, nor does it replace, the specific technical skills, knowledge, and abilities required to develop, administer, and defend the cyber environment. Rather it is a different and complimentary set of skills, knowledge, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm.

---

In the future, every  
military leader must be  
a cyber-strategic leader.

Service academies and war colleges in particular ought to play a key role in educating future and current members of the military on the unique aspects of cybersecurity, fusing knowledge, intellectual capacity, practical skills, and optimizing their campus-wide resources to devise comprehensive curricula that synthesize technical, policy, sociological, and legal components of the study of cybersecurity. In fact, as Soldiers, Sailors, Airmen, and Marines learn to turn their attention from incoming missiles to cyber weapons, a technology-centric education will be insufficient to counter and mitigate current and future cyber threats. Only a truly comprehensive education will help foster the requisite military leadership needed to fight and win in a deeply cybered and conflict prone world.<sup>[20]</sup>

Despite the pressing need to educate future cyber-strategic leaders across the whole range of social institutions and military services, few American universities, colleges, and academies offer courses or degree programs that combine cybersecurity technology, policy, law, economics, ethics, and other social sciences, and even fewer encourage collaboration among departments and other academic institutions to optimize their efforts and insights available for cross-fertilization.<sup>[21]</sup> Current cybersecurity programs, should be expanded and incorporated into all major technical and non-technical academic programs if we are to create a new cadre of cyber-strategic leaders spanning different sectors of society.

Efforts are already underway at military academies to educate and train select groups of students in information assurance, and cyber operations and to fill the ranks of the new

cyber corps. In 2012, for instance, service academies founded a “Military Academy Cyber Education Working Group,” which consists of members from the four main US service academies: the US Coast Guard Academy, the US Air Force Academy, the US Military Academy, the US Naval Academy, the Naval Postgraduate School, the Air Force Institute of Technology, US Cyber Command, and the National Security Agency (NSA). This group has sought to develop a body of knowledge for undergraduate cyber education for future officers, cyber leaders, and technical personnel.<sup>[22]</sup> Some of the academies are also involved in the Cyber Education Project (CEP), a other effort by computing professionals at different academic institutions to “develop undergraduate curriculum guidelines and a case for accreditation for educational programs in the cyber sciences.”<sup>[23]</sup> Despite these efforts, however, most of the existing academic programs remain highly technical and rarely pursue broader multi-disciplinary approaches commensurate with the complexity of cybersecurity. Indeed, there remains much to be done to fill this education gap and establish standardized core curricula in information technology and cybersecurity for all service academies.

What we need are the “academies of cybersecurity,” where different aspects of cyber-security are an integral component of any cadet, midshipmen, and officer’s military education and training, while also being fully integrated with more traditional missions. Service academies and professional military education are instrumental in creating a new cadre of cyber-strategic leaders. After all, these institutions are designed specifically to educate, train, and produce the future top military leaders and strategists who will have the skills, knowledge, and strategic acumen needed to take leadership roles on the battlefield, as well as in government agencies, and other military installations. There exists no group with a more urgent need for understanding cyber-related issues, honing the ability to lead, manage, and oversee cyber operations, and being prepared to act with little or no reliable information if adversaries are able to degrade or deny their access to cyberspace.<sup>[24]</sup>

### ***Methodology***<sup>[25]</sup>

This study summarizes current efforts by US service academies to include information technology or cybersecurity education in their curricula. It seeks to highlight those cyber components already present in updated curricula, review program effectiveness in promoting the study of cybersecurity and cyber warfare, and identify existing curriculum gaps in this field. This article does not provide an in-depth analysis of specific courses or an extensive audit of particular programs; rather, it offers an overview of the progress, or lack thereof, made by service academies to integrate information technology and cybersecurity into their programs and extracurricular activities.

The survey findings are based on data collected between November 2015 and February 2016. The data was obtained through a combination of interviews with service academy

faculty and staff, in addition to material drawn from their websites. The results stem from the responses to four main curriculum and extracurricular questions, and the use of a modified Likert approach<sup>[26]</sup> to evaluate the level of exposure students receive to cybersecurity issues in each of the service academies, and the opportunities offered to deepen their knowledge in the field. Respondents were asked whether their institution offered: 1) dedicated degree majors and/or core courses in information technology and cybersecurity; 2) elective courses in information technology and cybersecurity open to all students, regardless of major; 3) the possibility for cadets or midshipman to cross-register and enroll in other elective courses in information technology and cybersecurity at other schools; and 4) occasional seminars, conferences, war gaming exercises, or other training opportunities in cybersecurity and/or cyber operations. The modified Likert scale used to derive a notional ranking of the academies analyzed assigns a number (0 to 1) to each response as follows: “Yes” = 1; “Not specifically, but” = 0.5; “No” = 0. The answers are then added, and each service academy receives an overall score on a 0 to 4 scale, 4 being the highest score they can receive. The specific responses are also discussed in more detail in this article.

The authors assume that if a service academy requires all students to take at least one core course in ICT and cybersecurity, all cadets or midshipman will receive at least a basic understanding and the practical tools needed to manage the information security needs of their armed service and leverage ICTs for strategic advantage. If the academy offers elective courses in ICT or cybersecurity, cadets and midshipman interested in these topics will at least have the opportunity to explore the interlinkages between ICT, cybersecurity, and military readiness. If cybersecurity issues are covered as part of broader courses, we assume that students will gain a general understanding of the cyber challenges and opportunities specific to that field of study. Finally, if the academy offers occasional cyber-related seminars, conferences, war gaming exercises, visits to cyber units within different services, and the option of participation in cyber competitions, cadets and midshipman will have the opportunity to explore cybersecurity in more depth, and with a greater level of hands-on practicality. If none of these opportunities are provided, we assume that graduates of these programs do not gain a thorough understanding of the challenges, opportunities, and threats persistent in cyberspace beyond their own personal experience.

In addition, the study indicates whether the service academies have received the NSA/Department of Homeland Security (DHS) designation as a Center of Academic Excellence

---

There needs to be  
a concerted effort  
to develop a new  
generation of cyber-  
strategic leaders who  
will lead, manage,  
and oversee  
cyber defense.

in Information Assurance Education (CAE/IAE) and Research (CAE/R).<sup>[27]</sup> The goal of these programs is to reduce vulnerability in the national information infrastructure by promoting higher education and research in IA, and producing a growing number of professionals with IA expertise in various disciplines. Students attending designated schools are eligible to apply for scholarships and grants through the DoD Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.

SERVICE ACADEMIES SURVEY				
Service Academy	City	State	Likert Scale Average Score (Max = 4)	NSA/DHS Certification*
United States Air Force Academy	Colorado Springs	CO	3	CAE/IAE
United States Coast Guard Academy	New London	CT	2.5	N/A
United States Military Academy	West Point	NY	3.5	CAE/IAE
United States Naval Academy	Annapolis	MD	4	CAE/IAE

\* Indicates academy NSA/DHS designation as a Center of Academic Excellence (CAE) in Information Assurance Education (IAE) and/or Research (R).

United States Air Force Academy	Colorado Springs, CO
Likert Score: 3/4	NSA Cert: CAE/IAE

The Air Force was the first branch to recognize cyberspace as an operational domain, and to incorporate large portions of the Air Force’s intelligence units for network warfare along with the communications units under the 24th Air Force (a component of Air Force Space Command). This operational warfighting organization is tasked with executing full spectrum cyberspace operations.<sup>[28]</sup> Consequently, the US Air Force Academy (USAFA) incorporated some aspects of cybersecurity and cyber warfare education in its curricula, and has tried to align its offerings with the new career paths and fields created for Airmen.

Recently, USAFA instituted a new computer network security major designed specifically to help cadets better understand and gain proficiency in cyberspace.<sup>[29]</sup> The new major focuses on computer programming, embedded systems, networks, telecommunications, computer systems, computer investigations, and cyber operations. Although this program is highly technical and targeted at students aspiring to develop cyber expertise—either working in the cyber domain or becoming pilots with an in-depth knowledge of the software systems that underpin aircraft and weapons systems—students are also required to take one course on either strategy, political science, or cyber law. Moreover, the major includes a capstone project where students participate in a final hands-on exercise that includes red and blue team forces competing against military and external institutions, as Major Michael Chiaramonte explained.<sup>[30]</sup>

In addition, all cadets, regardless of their major, are required to take an Introduction to Computing course during their freshman year, which covers cybersecurity, cyber hygiene, cyber threats, and the supporting role of information technology in the planning and execution of national and military strategy. All cadets also take an electrical engineering course, which includes four lessons on cybersecurity. USAFA offers a few cyber-related electives, enabling students to delve deeper in other non-technical areas such as cybersecurity policy and politics, cyber law, military strategic studies, information and cyberspace operations, and, soon, digital forensics (the course is scheduled to start in Fall 2016). While the academy does not currently allow students to take additional courses on cybersecurity at other schools, they are considering offering this opportunity in a hybrid online format.

Moreover, cadets interested in this field can join the school's extracurricular cyber warfare club and the cyber competition team to gain further exposure to a variety of cyber threats facing military and government networks, and to get hands-on experience with simulated offensive and defensive cyber operations. Every year, students on the cyber team participate in numerous competitions and various capture the flag exercises against graduate students and professionals worldwide, frequently ranking among the top 10 percent of teams.

Finally, USAFA's Center of Innovation provides additional opportunities for some students to study malware and other complex computer security issues alongside faculty and researchers from Intel Corporation (the center serves as a testing ground for Intel Corporation's most promising new technologies).<sup>[31]</sup> The Center has recently started to explore how disruptive technology innovations can change the way the military operates, and how innovations in cyberspace can revolutionize cybersecurity for both the military and businesses.

From the information provided, all students at the Air Force Academy receive at least a basic foundation and understanding of information technology and cyber warfare during their freshman year, and have the opportunity to be further exposed to the cyber risks that



may impact mission capabilities and effectiveness through cybersecurity competitions and events. Those particularly interested in the study of cyberspace and cyber operations can pursue a Bachelor of Science degree in computer and network security. However, this is a challenging program that requires strong quantitative and analytical skills and a pre-disposition for computer programming. Given the time demands and stressors of academy life, only a limited number of dedicated students actively pursue this degree.

<b>United States Coast Guard Academy</b>	New London, CT
Likert Score: 2.5/4	NSA Cert: N/A

The US Coast Guard Academy (CGA) educates future leaders to serve in a multi-mission maritime force, tasked with providing critical services in protection of natural resources, maritime mobility, and national defense. A new core curriculum has recently been approved for the class of 2021, which will require all cadets, regardless of their major, to enroll in a cybersecurity fundamentals core course. However, at present, CGA only offers core courses with a cybersecurity focus for students in specific majors. For example, electrical engineering majors with a key competency in computers are required to take a Computer and Network Security course. The course expands on the skills, knowledge, and abilities acquired during the pre-requisite courses on Introduction to Computer Programming and Computer Communications and Networking, which introduce students to the fundamentals of computer and network security, including threats, vulnerabilities, exploits, intrusion protection systems, firewalls, cryptography, and mechanisms to mitigate risks. The course is also offered as an elective to electrical engineering majors with a systems emphasis. Students that partake in the course also have the opportunity to place “their education into practice as participants in the NSA’s annual Cyber Defense Exercise (CDX),” in which students from service academies design and build computer networks and defend them against intrusions by the NSA and the Central Security Service (CSS).<sup>[32]</sup> Likewise, students enrolled in the management major are required to take a Management Information Systems course, which prepares managers to function in a technological environment. Students are taught about the structure of information systems, management of computing technology, data processing, and information assurance.<sup>[33]</sup> Cadets can also choose to take two electives, either Information Technology in Organizations or Cybersecurity Crisis Management. The first elective provides students with an in-depth examination of fundamental technological and management issues relevant to information technology management in the Coast Guard, including computer architecture, network theory, and system administration.<sup>[34]</sup> The second course is a newly developed course, which “provides students with an interdisciplinary approach to understanding key systemic challenges associated with effective leadership and management of cyber-related incidents,” as Dr. Kimberly Young-McLear explained.<sup>[35]</sup> Although the course is offered in the management department, it is open to all majors. Topics include legal,

policy, network defense, business continuity planning, and risk management. The course also features guest speakers and lecturers from the Coast Guard and other governmental agencies. Students in the course, as well as selected students from other majors, have the opportunity to participate in a two-day cybersecurity seminar in Washington D.C. offered through the Coast Guard Academy's Institute for Leadership. During this field trip, cadets are provided cybersecurity guidance from senior government officials at the White House, Pentagon, Coast Guard Headquarters, and the National Cybersecurity and Communications Integration Center (NCCIC).

In addition, all students in their senior year are required to take a Public Management Consulting course, which provides students with an experience-based project to apply management and business principles, including cyber-related ones, to their final capstone. For instance, the management department has provided several opportunities for students to work on cybersecurity and information technology-related capstones. Clients have included DHS, Coast Guard Port and Facilities Compliance, and the Surface Forces Logistics Center.<sup>[36]</sup>

Other majors offer additional elective courses that cover some cybersecurity and/or information assurance topics as part of the broader course curriculum. For example, students in the government program have the option of taking an Intelligence and Democracy course, which examines various functions of intelligence from a human and technical perspective, and a Strategic Intelligence: Collection and Analysis course that explores how the Intelligence Community operates, from both a technical and human level.<sup>[37]</sup> Moreover, CGA participates in the Service Academy Exchange Program (SEAP) that allows cadets to participate in a semester-long exchange program with one of the other service academies. While this program is not specifically focused on cybersecurity, students could theoretically take a cybersecurity course offering at another academy to fulfill an elective requirement at CGA. Cadets also have the opportunity to take courses at the nearby Connecticut College to enhance the available offerings, as Dr. Kelly Seals explained.<sup>[38]</sup>

In 2015, CGA developed a new initiative to raise awareness among cadets of the importance of maintaining cybersecurity. The new cyber defense awareness training module is a three-day Cyber Range for all cadets to take part in during their second class summer. Cadets are trained in cybersecurity issues and have the opportunity to be exposed to live malware and experience the effects of poor cyber hygiene in a safe, segregated

---

---

Only a truly  
comprehensive  
education will help  
foster the requisite  
military leadership  
needed to fight and  
win in a deeply  
cybered and conflict  
prone world.



network environment.<sup>[39]</sup> The academy’s cadets have also recently formed a cyber team and participated in the annual CyberStakes competition, a DoD program originally launched by the Defense Advanced Research Projects Agency (DARPA) to build cyber proficiency in service academy midshipmen and cadets.<sup>[40]</sup> The CGA ‘hacking’ team offers cadets the opportunity to deepen their knowledge of computer networks while earning sports credits for their participation.<sup>[41]</sup>

Finally, the academy offers occasional conferences and guest lectures on cybersecurity. In the spring of 2015, for instance, the academy held a day-long cyber symposium with external cybersecurity experts from the military, government, academia, and industry. Topics ranged from cyber resiliency and the US maritime transportation system, to cyber intelligence policy, to insider threats.<sup>[42]</sup>

In brief, cadets at the Coast Guard Academy have the opportunity to be exposed to cybersecurity and information assurance through multiple extracurricular activities, and some courses depending on their major. CGA has recently made additional efforts to increase opportunities for cadets to acquire “the cybersecurity knowledge, skills, and abilities necessary to operate within the cyber domain and to be leaders in protecting maritime critical infrastructure and the maritime transportation system.”<sup>[43]</sup> As part of this effort, more courses could be offered outside of the electric engineering and management programs that explore the legal, ethical, economic, and policy implications of cybersecurity, and cadets could be encouraged to enroll or audit additional cybersecurity electives outside their major.

<b>United States Military Academy</b>	West Point, NY
Likert Score: 3.5/4	NSA Cert: CAE/IAE

The US Military Academy at West Point is dedicated to educating and training future Army officers with a focus on leadership development through academic, military, and physical education. All cadets are required to complete a core curriculum of 26 courses, which includes an introductory course in computing and information technology during their freshman year. While not entirely focused on cybersecurity, this course has a self-defense and protection focus and seeks to train students on mechanisms by which they can be responsible citizens in cyberspace. As the 2016 course catalog notes, the “core curriculum includes a computer science thread to ensure that every academy graduate is comfortable with and capable of using computers in an Army dependent on technology.”<sup>[44]</sup> Additionally, as part of the core curriculum, every cadet is required to select a core-engineering component that consists of three tailored engineering courses. One of the options is a cyber engineering sequence, which has become one of the more popular options among cadets.

West Point also has a number of computing and engineering majors that include substantive cybersecurity components. As Dr. Fernando Maymí explained, “although West Point does not offer a cybersecurity major, we strive to foster a cybersecurity focus within the population of cadets who are majoring in computer science, information technology, electric engineering, systems engineering, and mathematics.”<sup>[45]</sup> Students who are not majoring in one of these more technical majors are also required to take a second intermediate-level information technology course, which devotes a third of the classes to information assurance and security. The course culminates in a series of lessons that allow students to conduct computer reconnaissance, defense, and offense within a virtual network environment.<sup>[46]</sup> Furthermore, cadets can select a minor in cybersecurity, which includes courses in Cyber Security Engineering and Cyber Operations, among others. The cyber operations course offers a mature multi-disciplinary approach to cyber warfare, by covering the entire spectrum of legal, political, and ethical implications of information communication technology, cyber techniques, and attacks.<sup>[47]</sup> For cadets with an interest in cybersecurity, West Point also lines up a Senior Research Project (fall and spring semester) with a focus on software and systems development. The goal is that by the time those cadets graduate, typically about 15 per year, they will be ready to take operational assignments in this field.<sup>[48]</sup>

All students interested in cyber-related matters can take additional courses in technical disciplines or choose from a set of multi-disciplinary electives that include cyber warfare, law, ethics, digital forensics, and policy issues. This multi-disciplinary approach to the study of cybersecurity is the cornerstone of West Point’s strategy with the academy striving to include a stronger cyber component in most of its academic programs. While West Point does not offer students the ability to cross-register at other schools to include additional courses in cybersecurity in their curriculum, it does encourage students to apply for semesters abroad with a variety of foreign universities, and to participate in the SEAP exchange programs with another service academy. Theoretically cadets could augment their West Point education with courses in cybersecurity during their time abroad or through the SEAP program.<sup>[49]</sup>

Outside of formal course offerings, West Point offers a wide variety of extracurricular activities to enhance cadets’ experience and exposure to cybersecurity-related issues. For instance, the Cyber Research Center, housed in the Department of Electrical Engineering and Computer Science, provides research and educational opportunities for cadets and faculty to delve deeper into cyber-related subjects, including information assurance, information warfare, and forensics. The Center is involved throughout the year in annual cadet programs such as a cadet senior design capstone project management, an annual Cyber Defense Competition, cadet trip sections, annual summer internships, and cadet mentorships.<sup>[50]</sup> Cadets have the opportunity to participate in the Cadet Competitive

Cyber Team (C3T); a competitive academic team whose primary mission is to prepare for, and compete in, undergraduate cybersecurity competitions. C3T has participated in the Service Academy Cyber Stakes, sponsored by DARPA, and various capture the flag exercises, such as the 10th Annual NYU-Poly Cyber Security Awareness Capture the Flag competition.<sup>[51]</sup> In addition, a local chapter of the Association for Computing Machinery Security, Audit and Control (SIGSAC) Club is open to all students and provides cadets hand-on cyber experience in a secure (air gapped) environment.<sup>[52]</sup>

Moreover, West Point hosts a distinguished lecture series with cybersecurity luminaries, including senior military, and government officials and executive-level guest speakers from the US private sector, to discuss cyber threats to national security and the economy. Similarly, core and elective courses with a cybersecurity component often include guest lecturers. Those special lectures are usually scheduled during a common

---

West Point offers a wide variety of extracurricular activities to enhance cadets' experience and exposure to cybersecurity-related issues.

lecture hour so that participation can be opened to cadets that are not enrolled in those courses. For example, last year they hosted General Michael Hayden, former NSA and Central Intelligence Agency Director, and Dr. Chris Soghoian, Chief Technologist at the American Civil Liberties Union, for a discussion on privacy issues and bulk data collection.<sup>[53]</sup>

Finally, West Point is home to the Army Cyber Institute (ACI), whose mission is to develop intellectual capital and impactful cybersecurity partnerships for the Army and the nation to further cyberspace defense. Unlike the Cyber Research Center, the ACI is outward facing; they work with academia, government agencies, and industry in order to identify and build partnerships between individuals and organizations with cybersecurity challenges and potential solution sets.<sup>[54]</sup> The ACI runs a Cyber Leader Development (CLDP) program, which provides cadets an additional 800+ hours of impactful experiences outside the classroom through one-on-one mentorship, internships, conferences, clubs, and seminars. Cadets in CLDP have the opportunity to pursue advanced training—learning how to hack and defend networks—through SANS, Cisco, and other organizations during their spring break. CLDP includes field trips to the NSA, where cadets participate in a series of day-long discussions on cyberspace issues at the secret-level. At present, 160 cadets are enrolled in the program.<sup>[55]</sup>

The US Military Academy provides several opportunities for students to develop knowledge and skills in information technology and cybersecurity. West Point has taken a

multi-disciplinary approach to cybersecurity and recognizes the need for all military officers and decision-makers to have a basic understanding of the macro and micro implications of cyber issues. Despite their current efforts, however, cyber education has yet to be incorporated in all academic departments. Nonetheless, opportunity exists at West Point—particularly through the ACI—to deepen engagement with all faculty and departments, and offer additional cybersecurity and information assurance coursework in other academic focal areas (majors and minors). Moreover, as West Point develops more cybersecurity offerings, such as cyber ethics and cyber law, an inter-disciplinary major could be created that spans the technical and social science communities.

<b>United States Naval Academy</b>	Annapolis, MD
Likert Score: 4/4	NSA Cert: CAE/IAE

The US Naval Academy (USNA) provides academic and professional training for midshipmen that will become professional officers in the US Navy and Marine Corps. The academic programs at USNA are focused “especially on science, technology, engineering, and mathematics (STEM), in order to meet the current and future highly technical needs of the Navy.”<sup>[56]</sup> All midshipmen receive a Bachelor of Science upon graduation regardless of their major due to the technical content of the core curriculum.

In 2013, USNA became the first service academy, or university for that matter, to offer a dedicated Cyber Operations major at the undergraduate level, in addition to the more technical majors in Information Technology, Computer Science, and Computer Engineering. While fundamentals of the program will remain the same, the new Cyber Operations major has been designed to be updated and adapted over time as new technological innovations continue to develop, and to ensure students stay up to date with the latest technologies, explained Andrew Phillips, USNA Dean and Provost.<sup>[57]</sup> The Naval Academy’s Class of 2016 will be the first to graduate with the Cyber Operations degree. USNA was also the first of the service academies to require all students to take two mandatory courses in cybersecurity, an introduction during their freshman year, and a more in-depth elective that includes cyber policy and economics during their junior year. The two core courses provide a comprehensive overview of the principles behind the use, function, and operations of computers, networks, and applications with an emphasis on cybersecurity. “Both courses also include laboratory hours to emphasize some of the concepts into practical applications,” explained Captain Paul Tortora, Director of the USNA Center for Cyber Security Studies.<sup>[58]</sup>

Students interested in cyber-related issues can also choose from a variety of dedicated electives (regardless of their major), from more technical courses, such as Cyber Physical

Systems, Computer Networks with Security Applications, and Cryptology and Information Security, to more policy and strategy based, such as Cyber War Strategy, Information Technology and International Politics, Cyber Planning & Policy, Cyber Law & Ethics, Emerging Technologies, and Social Engineering, Hacktivism, and Info Ops in Cyber.<sup>[59]</sup> While most of these electives have prerequisites, the individual instructors can waive them should the student already possess the requisite knowledge.<sup>[60]</sup> Through these courses, students can gain a thorough understanding of the information system; the technical, social, policy, and institutional aspects of cybersecurity; the political and economic frameworks of cyber power; the legal and ethical challenges of cyber operations; the social engineering techniques and non-standard approaches employed by cyber threat actors to gain technical, military, economic, and intellectual advantages in cyberspace; and the effects of information technology on both the national and international political systems; and other aspects of the information revolution on the relations among nations. In addition, the cyber policy class runs a tabletop cyber exercise as part of the final class segment, both for students in Cyber Operations and Political Science, and International Relations majors.

Select senior students have an opportunity to cross-register at other schools to pursue additional cybersecurity courses, but only during their final/Spring semester. USNA has a Trident Scholar Program, which allows students to carry out independent study and local research, and a Voluntary Graduate Education Program (VGEP), which provides an opportunity for high-achieving midshipman to accelerate their undergraduate degree and take graduate classes at local elite universities, such as John Hopkins, Georgetown University, and the University of Maryland, during their final year. However, students must first finish all their undergraduate requirements and then be able to complete their graduate study within 7 months of graduation.<sup>[61]</sup> In addition, USNA enrolls about 10 to 15 students in SANS cybersecurity courses when available, typically during school breaks such as Spring Break or over the summer. Students majoring in Cyber Operations also have the opportunity to complete summer internships with civilian software and Internet companies as well as the NSA.

Beyond the classroom, midshipman can take advantage of the numerous cyber-related conferences, seminars, and small-scale cyber competitions hosted at the USNA. The Naval Academy also has a very active cyber competition team, which participates in a broad spectrum of cyber competitions, capture-the-flag events, and the annual NSA-sponsored CDX exercise. The USNA team won the last CDX exercise in the spring of 2015, and was recognized by President Obama at the White House, and also met with members of the National Security Council for cybersecurity discussions.<sup>[62]</sup>

USNA has also received \$120 million in federal funding and a \$1 million gift from Microsoft to build and equip a new cyber center (expected to be completed by late 2018)

that will feature 206,000 square feet of secure classrooms, research labs, lecture halls, state of the art technology, and the Academy's first Sensitive Compartmented Information Facility, or SCIF, a secure space that will allow for the discussion and management of classified materials.<sup>[63]</sup> The new building will be the home for the academy's Center for Cyber Security Studies, which provides support for the development of the cybersecurity curriculum, and for all the programs that contribute to knowledge, study, and research of cyber warfare at the USNA.<sup>[64]</sup>

Finally, USNA recently signed a new three-year, federally funded research partnership with the University of Maryland, Baltimore County, which will expand opportunities for both students and faculty to work on five major cybersecurity projects, including research to: detect hacks; strengthen the security of cloud-storage systems; develop hardware to detect anomalies and signal breaches; fortify defenses of social-media systems; and protect cell phones without burdening users.<sup>[65]</sup>

All midshipmen at the US Naval Academy receive at least a basic understanding of the full spectrum of cybersecurity issues from technical to strategic leadership, and the

---

Only then will this new cadre of cyber-strategic military leaders be able to harness the right tools, people, strategies, and balance of offensive and defensive capabilities.

practical knowledge needed to integrate cyber capabilities and cyber operations with the broader needs and missions of the US Navy. In fact, although the core curriculum at the USNA seems highly focused on science and technology, it has actually incorporated a significant number of policy, legal, sociological, and institutional components to the study of cybersecurity. Together with the more technical aspects of cybersecurity, the various programs and extracurricular activities at the Naval Academy are preparing

the next generation of cyber-strategic leaders for the Navy and a select group of naval officers with an in-depth expertise and experience in cybersecurity and cyber warfare. In addition, the academy's location in Maryland—a valued contributor to national cybersecurity and a trendsetter among states leading the cyber pack—and its proximity to the state's world-class educational institutions, leading federal assets, and a dynamic private sector are providing students and faculty additional research, training, and educational opportunities in this field.<sup>[66]</sup> Despite the clear strengths of the USNA programs, continuous emphasis should be placed on integrating an even more robust cybersecurity component into broader midshipman coursework.




### *Conclusion and Future Direction*

The use of ICTs has become the most dominant trend in interstate competition in the 21st century, whether in times of peace, tension, or open conflict. ICTs have become the foundation of modern militaries—from the hardware and software that underpin all military platforms, to the communication systems used to move information to commanders and troops, to the digital devices needed to control weapons systems, assure situational awareness, gather intelligence, and project force. Today, no modern military can enter the battlespace without some reliance on ICTs and cyberspace.

Given this undeniable and critical reliance on cyberspace for achieving military success, all future military leaders must be comfortable operating in this space, from both a human and technical perspective, and understand the challenges, threats, and opportunities it presents. Strong cybersecurity skills, the ability to obtain, process, analyze, manipulate, and correlate data, and the knowledge necessary to leverage cyberspace for strategic advantage will be the deciding factor for military success and resiliency. For these reasons, every future military leader must be a cyber-strategic leader. These individuals need not have specific training in engineering or programming, but must be equipped with a deep understanding of the cyber context in which they operate, combined with an appreciation of military ethics, law, strategic studies, political theory, organizational theory, international relations, and additional sciences. Only then will this new cadre of cyber-strategic military leaders be able to harness the right tools, people, strategies, and balance of offensive and defensive capabilities.

Military academic institutions, both at the undergraduate and graduate level, must be the incubators of future cyber-strategic leaders. This survey has highlighted an increased effort by the US service academies to develop new content for cybersecurity education at the undergraduate level, include cyber components in existing curricula and extracurricular activities, and prepare cadets and midshipman to lead in an age of persistent cyber threat. These efforts are commendable, especially in comparison to the much slower or nonexistent integration of cybersecurity components in undergraduate programs across American civilian universities. Despite these laudable developments, however, the survey has also shown that more progress is still needed to educate all future military officers about the complexities of cybersecurity. Many of the service academies already provide cyber-related coursework for students pursuing more technical career paths. These efforts, however, must extend to all students, both in technical and non-technical career paths. Moreover, classroom study is only part of the equation. Extracurricular activities provide cadets and midshipman valuable hands-on experience. Cybersecurity-related internships and clubs can increase students' professional network, develop their cyber expertise, and provide them with opportunities to implement classroom lessons-learned in a real world environment. These activities should be expanded to cater to technical and non-techni-

cal students. In so doing, the service academies will reorient their educational objectives and outcomes to better reflect the reality of the modern battlefield. By equipping all their graduates with the knowledge necessary to confront a wide array of cyber threats, the service academies will play a vital role in ensuring that the US military is able to establish both a competitive and security advantage on this new and increasingly critical “battlespace.” 

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*



## NOTES

1. Martin C. Libicki, "Crisis and Escalation in Cyberspace," *RAND Project Air Force* (2012), and Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Arlington, VA: Cyber Conflict Studies Association, 2013).
2. "Middle Class Economics," *The President's Budget Fiscal Year 2016*, August 7, 2015, [https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact\\_sheets/cybersecurityupdated.pdf](https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurityupdated.pdf)
3. "The Department of Defense Cyber Strategy," *US Department of Defense* (April 2015), 4-5.
4. For an overview of military readiness, see: Todd Harrison, "Rethinking Readiness," *Strategic Studies Quarterly* 8.3 (Fall 2014).
5. Rep. Jim Langevin, "Column: Cyber dominance meaningless without skilled workforce," *Federal News Radio*, October 12, 2012, <http://federalnewsradio.com/congress/2012/10/column-cyber-dominance-meaningless-without-skilled-workforce/>.
6. While the authors recognize that there are other academic institutions training students who will be commissioned in the US military, the study focuses solely on the four main US service academies: US Coast Guard Academy, US Air Force Academy, US Military Academy, and US Naval Academy, because these academic institutions are designed exclusively for the purpose of commissioning future military officers into their respective services. For instance, while the US Merchant Marine Academy is a federal service academy whose graduates may accept a commission in the US military, this academic institution is primarily charged with training personnel for the US merchant marine; a fleet of US civilian and federally owned merchant ships managed by the government or private sector. Students here can, however, choose to commission into a branch of the military after graduation.
7. Francesca Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," *Pell Center Report*, (August 7, 2013), 1.
8. Department of Defense, "Cyber Operations Personnel Report," *Report to the Congressional Defense Committees* (April 2011).
9. "Pentagon's Cyber Mission Forces Takes Shape," *Federation of American Scientists*, September 10, 2015, <https://fas.org/blogs/secrecy/2015/09/dod-cmf/>, and "Middle Class Economics," *The Presidents Budget Fiscal Year 2016*, August 7, 2015, [https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact\\_sheets/cybersecurity-updated.pdf](https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity-updated.pdf).
10. William Welsh, "Cyber warriors: the next generation," *Defense Systems*, 23 January 2014, <https://defensesystems.com/Articles/2014/01/23/Next-generation-cyber-warriors.aspx?Page=1>. For an overview of the current state of CMF recruitment and training, see: Bill Matthews, "Military Battles to Man its Developing Cyber Force," *GovTech Works*, September 16, 2015, <https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/>.
11. "Jennifer J. Li and Lindsay Daugherty, "Training Cyber Warriors: What Can Be Learned from Defense Language Training," *RAND* (2015), ii.
12. Secretary of Defense Speech, "Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," *US Department of Defense*, April 23, 2015, <http://www.defense.gov/News/Speeches/Speech-View/Article/606666>.
13. Robert M. Gates, "Department of Defense Strategy for Operating in Cyberspace," *US Department of Defense*, (July 2011), 1.
14. Daniel Goure, "Six Steps to Securing DoD's Networks for the 21st Century," *Real Clear Defense*, 12 August 2015, [http://www.realcleardefense.com/articles/2015/08/12/six\\_steps\\_to\\_securing\\_dods\\_networks\\_for\\_the\\_21st\\_century\\_\\_108352.html](http://www.realcleardefense.com/articles/2015/08/12/six_steps_to_securing_dods_networks_for_the_21st_century__108352.html).
15. If tampered, malicious microelectronics or chips underlie weapons platforms, they can operate as hidden "back doors" for espionage or sabotage. Malicious hardware, in fact, can be inserted into a chip after the design phase, but prior to its fabrication, thus making it challenging to detect. This is a risk for all weapons platforms, including those that are "air-gapped" or "off the grid." For more information on the use of microelectronics in modern military platforms, see: Jennifer McArdle, "Hardware Security in the US-Indian Cyber Dialogue," *The National Interest*, June 30, 2014, <http://nationalinterest.org/feature/hardware-security-the-us-indian-cyber-dialogue-10770>, and Defense Science Board, "High Performance Microchip Supply," *Task Force Report* (2005).

## NOTES

16. Authors' interview with Dr. Fernando Maymí, Deputy Director of the Army Cyber Institute at West Point and Assistant Professor in the Department of Electrical Engineering and Computer Science, December 14, 2015.
17. Spidaleri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.
18. National Research Council, "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," *The National Academic Press* (Washington, D.C.) 2014.
19. Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bringing from Concept to Cyber Superiority," *Joint Force Quarterly* 68, no.1 (January 2013), 53-58.
20. *Cybered conflict* differs from *cyber war* or *cyber battle*. The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. "Cybered conflicts are those nationally significant aggressive and disruptive conflicts for which seminal events determining the outcome could not have occurred without 'cyber' (meaning networked technologies) mechanisms at critical junctures in the determining course of events." Chris C. Demchak, "Resilience, Disruption, and a 'Cyber Westphalia:' Options for National Security in a Cybered Conflict World," in Nicholas Burns and Jonathon Price, eds., *Securing Cyberspace: A New Domain for National Security*, The Aspen Institute (Washington, D.C.), 63.
21. "Francesca Spidaleri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," *Pell Center Report*, (March 26, 2013), 3.
22. Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor, "Cyber Education: A Multi-Level, Multi-Discipline Approach," *US Military Academy*, (September/ October 2015), 44.
23. "Cyber Education Project," <http://www.cybereducationproject.org>.
24. Spidaleri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.
25. This methodology is adapted from a methodology developed and employed in 2013 to assess military graduate programs that offer Joint Professional Military Education (JPME). The results provided an overview of the efforts by JPME institutions to include information technology and cybersecurity into their curricula. For more information, see: Spidaleri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," 2013.
26. The Likert scale is commonly used in survey research. This approach is usually used to measure respondent's attitudes by asking the extent to which they agree or disagree with a particular question or statement.
27. NSA and DHS set up criteria for the designation of universities or academic departments, both civilian and military, as Center of Academic Excellence in Information Assurance Education (CAE/IAE) and Research (CAE/R). The designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation. The list of CAE academic institutions can be found at: [https://www.nsa.gov/ia/academic\\_outreach/nat\\_cae/institutions.shtml](https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml).
28. "24th Air Force Fact Sheet," <http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663>.
29. Don Branum, "Academy Introduces Computer Network Security Major," *US Air Force*, August 12, 2014, <http://www.af.mil/News/ArticleDisplay/tabid/223/Article/494118/academy-introduces-computer-network-security-major.aspx>.
30. Authors' interview with Major Michael V. Chiamonte, Assistant Professor, Department of Computer Science, US Air Force Academy, December 9, 2015.
31. "Center of Innovation," *US Air Force Academy*, <http://www.usafa.edu/df/dfe/dfer/centers/coi/>.
32. "Catalog of Courses (2015-2016)," *US Coast Guard Academy*, 52-54 and 92. The Central Security Service is a DoD agency established to integrate the NSA and the Service Cryptologic Elements (SCE) of the US Armed Forces in the field of signals intelligence, cryptology, and information assurance at the tactical level. For more information, see: National Security Agency/Central Security Service, [https://www.nsa.gov/about/central\\_security\\_service/css\\_insignia.shtml](https://www.nsa.gov/about/central_security_service/css_insignia.shtml).
33. "Catalog of Courses," *US Coast Guard Academy*, 80 and 154.
34. *Ibid*, 80 and 157. For more information on course, see also: LCDR Joseph Benin and CDR Kelly Seals, "Rising to Today's Challenges: Cyber Education and Training at the Coast Guard Academy," *Around the Academy* (October 2015), 35-36.

## NOTES

35. Authors' interview with Dr. Kimberly Young-McLear, Coast Guard Lieutenant and member of the Permanent Commissioned Teaching Staff, February 27, 2016.
36. *Ibid.*
37. "Catalog of Courses," US Coast Guard Academy, 69 and 110-111.
38. Authors' interview with Dr. Kelly Seals, Coast Guard Commander and Section Chief and Program Chair for the Electrical Engineering Department, February 26, 2016.
39. Joseph Benin, "US Coast Guard Academy host cyber symposium," *The Coast Guard Blog for Maritime Professionals*, April 24, 2105, <http://mariners.coastguard.dodlive.mil/2015/04/24/4242015-u-s-coast-guard-academy-hosts-cyber-symposium/>, and LCDR Joseph Benin and CDR Kelly Seals, "Rising to Today's Challenges: Cyber Education and Training at the Coast Guard Academy," *Around the Academy* (October 2015), 38-40.
40. Cheryl Pellerin, "Service Academy CyberStakes Proves Worth as Learning Tool," *US Department of Defense*, February 16, 2016, <http://www.defense.gov/News-Article-View/Article/656181/service-academy-cyberstakes-proves-worth-as-learning-tool>.
41. Julia Bergman, "Cyber team forms at the Coast Guard Academy," *The Day*, January 17, 2016, <http://www.theday.com/article/20160117/NWS09/160119264>.
42. "Coast Guard Academy Cyber Symposium," *US Coast Guard Academy Symposium Agenda*, March 26, 2015.
43. Benin and Seals, "Rising to Today's Challenges," (2015), 34.
44. Office of the Dean, "Academic Program, Class of 2017: Curriculum and Course Descriptions," *US Military Academy West Point* (2016), 18.
45. Fernando Maymí, authors' interview, 2015.
46. Sobieski et al., "Cyber Education: A Multi-Level, Multi-Discipline Approach," (2015): 45.
47. Office of the Dean, "Academic Program, Class of 2017" (2016), 131.
48. Fernando Maymí, authors' interview, 2015.
49. *Ibid.*
50. "Welcome to the Cyber Research Center," *US Military Academy*, <http://www.usma.edu/crc/SitePages/Home.aspx>, and authors' interview with Dr. Fernando Maymí, 2015.
51. Cadet Competitive Cyber Team, C3T," *US Military Academy West Point*.
52. Sobieski et al., "Cyber Education: A Multi-Level, Multi-Discipline Approach," (2015), 46.
53. Fernando Maymí, authors' interview, 2015.
54. *Ibid.*
55. "Cyber Leader Development Program (CLDP) Overview," *US Military Academy*, <http://www.usma.edu/acc/SitePages/CLDP.aspx>, and authors interview with Dr. Fernando Maymí, 2015.
56. "Academics: Majors," *US Naval Academy*, <http://www.usna.edu/Academics/Majors-and-Courses/index.php>.
57. Mike Hoffman, "Naval Academy Launches Cyber Operations Major," *Defense Tech*, June 8, 2013, <http://www.defense-tech.org/2013/06/08/naval-academy-launches-cyber-operations-major/>.
58. Authors' interview with Captain Paul Tortora, Director of the USNA Center for Cyber Security Studies, November 23, 2015.
59. "Academics: Course Listing," *US Naval Academy*, <http://www.usna.edu/Academics/Majors-and-Courses/course-description/All-Courses.php>.

## NOTES

60. Paul Tortora, authors' interview, 2015.

61. *Ibid.*

62. Nathan Wikes, "USNA Midshipmen Recognized by President Obama for Achievement," *Official Website of the US Navy*, May 7, 2015, [http://www.navy.mil/submit/display.asp?story\\_id=86982](http://www.navy.mil/submit/display.asp?story_id=86982).

63. Meghann Myers, "Naval Academy gets \$120 million for new cyber center," *Navy Times*, December 18, 2014, <http://www.navytimes.com/story/military/capitol-hill/2014/12/18/naval-academy-annapolis-cyber-building/20592213/>, and "Microsoft Supports Naval Academy's Center for Cyber Security Studies Building with Gift of \$1Million," *PR Newswire*, September 24, 2015, <http://www.prnewswire.com/news-releases/microsoft-supports-naval-academys-center-for-cyber-security-studies-building-with-gift-of-1-million-300148581.html>.

64. "Center for Cyber Security Studies," *US Naval Academy*, <http://www.usna.edu/CyberCenter/>.

65. Tim Prudente, "Naval Academy, UMBC partner to develop cyber security defenses," *Capital Gazette*, September 27, 2015, [http://www.capitalgazette.com/news/naval\\_academy/ph-ac-cn-cyber-security-0926-20150924-story.html](http://www.capitalgazette.com/news/naval_academy/ph-ac-cn-cyber-security-0926-20150924-story.html).

66. Francesca Spidalieri, "State of the States on Cybersecurity," *Pell Center Report* (November 2015), 14, <http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf>.



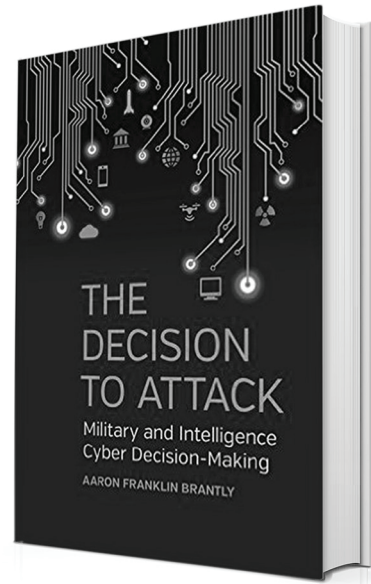
# THE CYBER DEFENSE REVIEW

◆ BOOK REVIEW ◆



The Decision to Attack:  
Military and Intelligence  
Cyber Decision-Making  
by Aaron F. Brantly

Reviewed by Dr. Jan Kallberg



Dr. Aaron Brantly's book *The Decision to Attack: Military and Intelligence Cyber Decision-Making* is timely, and addresses the question why states engage in cyber operations or not. One strength of this book is that Brantly explains the foundation for his decision-making and behaviors model. This early explanation of the model helps the reader understand which lens the author used for his research, and also puts the findings in a broader context. Brantly uses a rational choice decision-making model based on Bruce Bueno de Mesquita's development of an expected utility theory. A reader might suggest another theory or question the proper use of the utilized model due to states' inability to fully understand the contested space and lack of information, which are valid concerns, but it does demonstrate a gap in cyber decision-making literature that needs to be filled by relevant scholarship. In reading today's scholarly cyber literature, there are few attempts to theorize the decision-making process at the political and strategic level.

Dr. Brantly puts great emphasis on explaining and visualizing how traditional state decision-making applies in cyberspace, but also presents cyber characteristics that undermine the ability to use traditional international relations concepts and decision-making theory. As an example, Bruce Bueno de Mesquita's theory for state conflict is based on open conflicts and coalition-building, meanwhile in the cyber domain, for now, the central struggles are covert with each state a solitary actor. Brantly explains the cyber developments leading to today's complicated cyber landscape, and lays out the structure and intent with this informed study.



Chapter 2 seeks to answer two questions—“why is cyber important to national security?” and “why is the cyber domain inherently asymmetric?”, and to explain cyber behavior. These two questions are pivotal to this study, and Brantly superbly answers them. He distills out these two questions, which are often ignored in other political science books and research papers—why does cyber matter and why is it different? The key parts of Brantly's arguments are clearly visible and not hidden in an abundance of words and lengthy paragraphs, which makes it an easier read for those of us interested in the cyber field.

The cogent presentation of arguments supports a reader seeking to learn and participate in the cybersecurity conversation. The explanations and the answers are fully comprehended, and we are able to quickly grasp the question. I think this is a strength in Brantly's authorship. Once the reader grapples with the model, and starts to assess one's own variables and values, Brantly's easily understood methods on how to feed the model and view the results invite the reader to challenge Brantly and run the experiment themselves. As a reader, I find the invitation to bring your own data and run the test with Brantly's model intellectually inviting. Brantly's *The Decision to Attack: Military and Intelligence Cyber Decision-Making* fills a critical gap in the literature and is a multifaceted book as it both explains the concepts of cyber, puts cyber in a national security decision-making context, and allows you to test your own assumptions. It is an enjoyable and important read. 🛡️

---

### *The Decision to Attack: Military and Intelligence Cyber Decision-Making*

Author: Aaron F. Brantly

Publisher: University of Georgia Press (April 15, 2016)

Series: Studies in Security and International Affairs

Hardcover: 248 pages

Language: English

ISBN-10: 0820349208

ISBN-13: 978-0820349206

Price: \$49.95 hardcover

*The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.*



---

THE ARMY CYBER INSTITUTE IS A NATIONAL RESOURCE FOR RESEARCH, ADVICE AND EDUCATION IN THE CYBER DOMAIN, ENGAGING ARMY, GOVERNMENT, ACADEMIC AND INDUSTRIAL CYBER COMMUNITIES TO BUILD INTELLECTUAL CAPITAL AND EXPAND THE KNOWLEDGE BASE FOR THE PURPOSE OF ENABLING EFFECTIVE ARMY CYBER DEFENSE AND CYBER OPERATIONS.