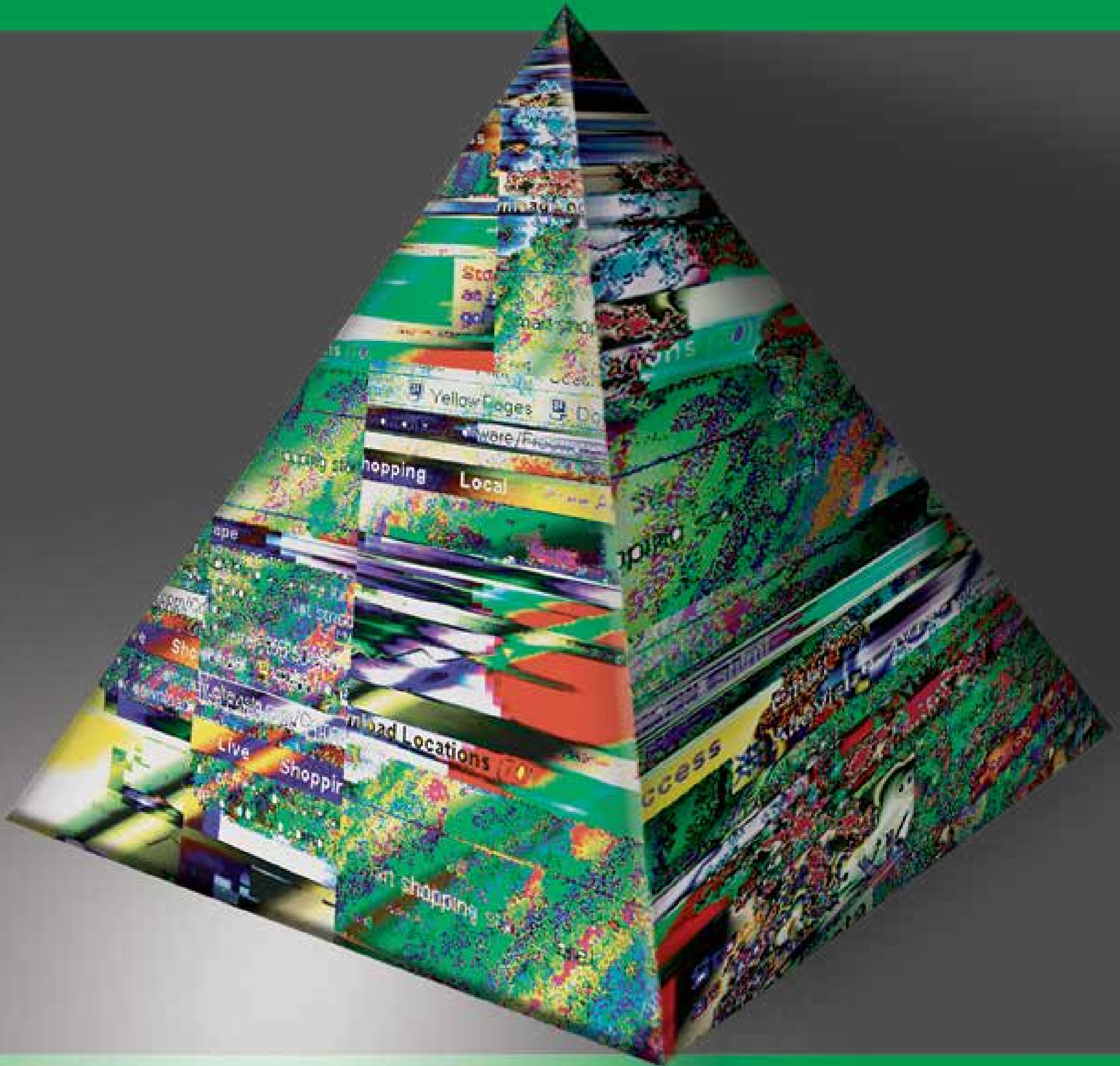
PRISM

VOL. 7, NO. 2 | 2017

THE FIFTH DOMAIN



A JOURNAL OF THE CENTER FOR COMPLEX OPERATIONS

PRISM

VOL. 7, NO.2 2017

EDITOR

Mr. Michael Miklaucic

DEPUTY EDITOR

Ms. Patricia Clough

WEBMASTER

Ms. Rebecca Harper

DESIGN

Ms. Jamie Harvey,
U.S. Government Publishing Office

EDITORIAL ASSISTANTS

Ms. Eva Kahan
Mr. Sven Stauder
Mr. Carlton Haelig

PUBLISHER

Dr. Joseph J. Collins

ISSN 2157–0663

ABOUT

PRISM, a quarterly journal published by the Center for Complex Operations (CCO) at National Defense University, aims to illuminate and provoke debate on whole-of-government efforts to conduct reconstruction, stabilization, counterinsurgency, and irregular warfare operations. Since its inaugural issue in 2010, *PRISM*'s readership has expanded to include more than 10,000 officials, servicemen and women, and practitioners from across the diplomatic, defense, and development communities in more than 88 countries.

COMMUNICATIONS

PRISM encourages authors to aggressively seek out and identify problems that should be addressed irrespective of prevailing U.S. Government policy or current military doctrine. We welcome unsolicited manusscripts from policymakers, practitioners, and scholars, particularly those that present emerging thought, best practices, or training and education innovations.

Please direct editorial contributions to the link on the CCO website or to the addresses below. If you choose to mail a hard copy, please provide a phone number and email for feedback.

Editor, *PRISM*
260 Fifth Avenue, S.W.
Fort Lesley J. McNair
Washington DC 20319

SUBJ: Manuscript Submission
<prism@ndu.edu>

Submissions will be reviewed by the *PRISM* editorial staff, who reviews material on a rolling basis. Publication threshold for articles and critiques varies but is largely determined by topical relevance, continuing education for national and international security professionals, scholarly standards of argumentation, quality of writing, and readability. To help achieve threshold, authors are strongly encouraged to recommend clear solutions or to arm the reader with actionable knowledge.

PRISM's review process can last several months. The staff will contact you during that timeframe accepting or regretfully rejecting the submission. If the staff is unable to publish a submission within four months of acceptance, *PRISM* will revert publication rights to the author so that they may explore other publication options.

DISCLAIMER

This is the authoritative, official U.S. Department of Defense (DOD) edition of *PRISM*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *PRISM* should be acknowledged whenever material is quoted from or based on its content.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of DOD or any other agency of the Federal Government, or any other organization associated with this publication.

SUBSCRIPTIONS

PRISM is provided as an educational public service. Please visit the CCO website to subscribe. Should your address change, please email the editorial staff at the address listed above.

COVER ART

Image is a derivative of "Teo Spiller computer graphic image from 1997" by Cacophonia Artwork. From <https://commons.wikimedia.org/wiki/File:CYber_Graphic.jpg>. Licensed under CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0/deed.en>.

NDU'S CENTER FOR COMPLEX OPERATIONS

The United States Congress in 2009 authorized the establishment of a Center for Complex Operations (CCO) in response to a widely perceived need for interagency interoperability in analysis of, planning for, and intervening in complex operations worldwide. These include reconstruction, stabilization, counterinsurgency, and irregular warfare—operations that demand support from all elements of national power to succeed.

Created within DOD as a collaborative initiative with support from the Department of State and the U.S. Agency for International Development, the aim of CCO is to:

- enable more effective networking, coordination, and synchronization of preparations for deployment of U.S. Government (USG) personnel for complex operations;
- compile best practices and lessons learned;
- identify training and education gaps, and then facilitate efforts to fill those gaps;
- and to serve as a feedback and information conduit to senior U.S. leaders within the defense, diplomacy, and development arenas.

PRISM is tailored to serve policymakers, scholars, and practitioners working to enhance USG competency in complex operations.

FEATURES

INTERVIEW

BOOK REVIEWS

Integrating cyber and electronic warfare capabilities increases the commander's situational awareness. (U.S. Army)

Prologue

Nearly a half century ago in October 1969, computer programmers at the University of California, Los Angeles used a primitive Department of Defense computer network called ARPANET to send the first messages to computers at Stanford Research Institute. This quiet event, considered by some to be the birth of the internet, ignited a technological movement within the computer and information industries that eventually transformed the world into a globally connected society utterly dependent on instant access to information, yet increasingly vulnerable to network intrusions by those who seek to steal sensitive data or disrupt cyber infrastructure.

This dependence and vulnerability is perhaps most prominent in the U.S. military. The information that moves through our networks empowers our forces in the field, enabling operators to make tactical and operational decisions, often with life-or-death consequences, that affect a strategic outcome. The Joint Force's ability to collect cues, understand and use big data to make decisions quickly, and then communicate those decisions to our fielded forces is an asymmetric advantage. But it is not a birthright or guaranteed to last. The daily attacks on our networks are increasingly sophisticated. A legion of cyber professionals relentlessly defends our networks from those who wish us ill, but we cannot win cyber defense by having humans react to intrusions at human speed. We must empower machines to monitor and defend the networks at machine speed while providing options for humans to make decisions. Otherwise, we risk giving our opponents maneuvering space in that domain. We still have much work to do in this area.

In addition to human-machine teaming, we need to continue investing in and developing a more effective framework for deterring cyberattacks, attributing intrusions, and managing escalation. Part of the solution lies in how we organize, train, and equip the cyber workforce. The creation of the Department's 133 cyber mission force teams and the elevation of United States Cyber Command to a unified combatant command are steps in the right direction, as both efforts will enhance the Joint Force's ability to deny, withstand, or respond to attacks on our systems or supporting infrastructure. Other key elements include sharing information with the Intelligence Community, our allies, and our partners to reduce the anonymity of malicious actors; deconflicting cyberspace operations among the dozens of U.S. cyber organizations and the interagency; and integrating cyber requirements into operational planning and execution. It will take continued investment in our warfighters and the capabilities they employ to maintain our strategic edge in cyberspace. We have no choice; the role of cyberspace in U.S. national security will only continue to grow.

These are just a few of the challenges and opportunities facing the nation in the cyber domain that you will find in this issue of *PRISM*. The articles by these senior leaders, strategic thinkers, and cyber experts are timely, relevant, and of interest to both professional cyber warriors and what I call pedestrian cyber users—everyone who uses a computer. I encourage you to read each article with a critical eye to discover ways we can improve how we share information, use big data to aid decisionmaking, and defend our networks.

General Paul J. Selva
Vice Chairman of the Joint Chiefs of Staff

A systems administrator from the Air Force Technical Applications Center's (AFTAC) Cyber Capabilities Squadron troubleshoots a lost server connection to keep AFTAC's nuclear treaty monitoring mission going strong. (U.S. Air Force/Susan A. Romano)

Cognitive-Emotional Conflict

Adversary Will and Social Resilience

By Linton Wells II

Today's information sharing tools let adversaries interfere more directly than ever with a targeted nation's political processes and the minds of its citizens.[1] Operating effectively in such "cognitive-emotional conflict" requires that information-based capabilities be employed and countered in agile, integrated ways across the military, government, and society.[2] Coherent narratives tied to strategy and backed by actions are important.[3] Technical cyberspace activities need to be well-coordinated with content-based approaches like military information operations, government-wide messaging, and intelligence gathering (including all forms of security).[4] Even more important is to build a society's resilience against persistent, disruptive, or disinformation campaigns that aim to undermine citizen confidence and core beliefs.[5]

The need for effective messaging is nothing new—targeting the minds of opposing leaders and the morale of their forces has been central to warfare from time immemorial. Historically, galvanizing public opinion in democracies usually has taken dramatic acts, from the Boston Massacre, to Pearl Harbor, to 9/11. Less dramatically, waning public opinion led President Bush to the Surge in Iraq, and President Obama to adjust his approach in Afghanistan. Activists today, however, have much more direct access to growing numbers of citizens, either to advocate for positions, muddy the waters of public opinion with alternative facts and fake news, or leak secrets to wide audiences. Empowered individuals and small groups can leverage media to enhance their impact by ensuring their asymmetric actions against people, societal structures, or military forces are much more widely disseminated. Some information activities will involve cyberspace operations, while some will involve more traditional information means. In any case, government communication tools such as press releases, white papers, web posts, or even leadership speeches rarely are effective counters to these information flows, especially when poorly coordinated.

The U.S. military and intelligence communities are starting to integrate their capabilities better, but implementing whole-of-government approaches is proving much harder owing to diverse interests, capabilities, and understandings of the information environment. Strengthening society's overall resilience to such campaigns is

Dr. Linton Wells II is a Visiting Distinguished Research Fellow at National Defense University. A retired U.S. Navy officer with more than five decades of public service, Dr. Wells served as Deputy Under Secretary of Defense and twice as Principal Deputy Assistant Secretary of Defense.

even more difficult, and also more important. A variety of reasons, from lack of trust to lack of capability, make it hard for most Western governments to craft and promote effective resilience campaigns. That said, transparency ultimately is a powerful asset, and where checks and balances, horizontal information flows, and citizen engagement exists, societies can adapt and become more resilient to cognitive-emotional attacks. However, the Strategic Multi-Layer Assessment (SMA) and others are doing important work on fake news inoculation and enhancing population resilience, as well as the use of neuroscience to help understand subconscious decisionmaking.[6] Positive steps to reframe and refocus arguments can be used to counter disinformation campaign tactics.[7]

The Continuum of Conflict

Where does cognitive-emotional conflict fit into the broader continuum of conflict that exists today? First one must define the continuum. Strategist Frank Hoffman at National Defense University defines this as measures ranging from "short of armed conflict" to "major theater war."[8] The spectrum includes an "unconventional and special warfare" category that cuts across the entire continuum of violence.[9] Most of the conflicts today fall into the blue and green zones identified in Figure 1.

Measures Short of Armed Conflict

A proposed definition is the employment of covert or illegal activities that are below the threshold of violence. This includes disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of jurisprudence, and financial corruption as part of an integrated design to achieve strategic advantage.[10]

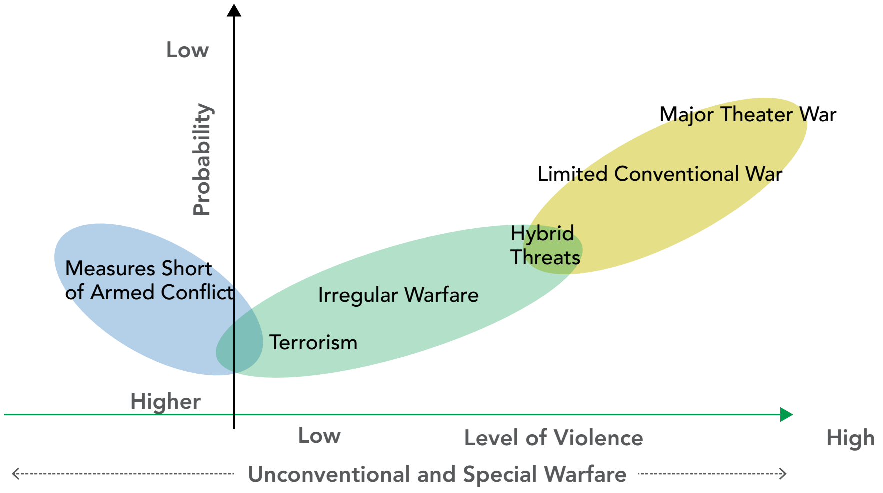
Irregular Warfare and Terrorism

Existing U.S. doctrine defines irregular warfare as a "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations."[11] Irregular warfare is characterized by indirect and asymmetric approaches that avoid direct and risky confrontations with strong forces.[12] Irregular warfare may include criminal activity and/or terrorism.

Hybrid Threats

Hoffman defines this group as the "tailored violent application of advanced conventional military

FIGURE 1: Continuum of Conflict.



capabilities with irregular tactics, or combination of forces during armed conflict."[13]

Theories of Conflict and Resilience

War is "an act of force to compel the enemy to do your will"—fair enough, but a complementary formulation is "… supreme excellence [in war] consists in breaking the enemy's resistance without fighting."[14] Within the continuum of conflict, breaking the resistance of *both* civilian and military adversaries without fighting major wars is an increasingly common objective.

Key arguments in this area were introduced by John Arquilla and David Ronfeldt in their 1993 article "Cyberwar is Coming!"[15] that first introduced the concept of "cyberwar"—"the idea that the vulnerability of communications could cripple an advanced army" by "disrupting, if not destroying, information and communication systems…on which an adversary relies in order to *know itself*…[16] Cyberwar has proven hard to define, and is not included in the official U.S. military lexicon, but "cyberspace operations" are, and they are associated with powerful technical components, usually considered to be offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and computer network exploitation (CNE).[17] Such operations can impact most conflicts, but often they have been treated as technical capabilities injected from a parallel, networked universe, rather than integrated as part of an overall campaign. However, Arquilla's and Ronfeldt's seminal 1993 article not only discussed how the information age is altering the nature of all conflict, but also introduced the concept of "netwar" in which actors seek to "disrupt, damage, or modify what a target population knows or thinks it knows about the world around it."[18] Today cyberspace operations closely relate to cyberwar with potential impacts on military systems, critical infrastructures, etc., while netwar is increasingly relevant to the cognitive and emotional disruption of societies.[19]

Worldwide, hundreds of billions of dollars are spent to defeat enemies on high-intensity battlefields. Such capabilities are necessary, but insufficient. A variety of cognitive-emotional campaigns are underway, from sustained efforts to undermine respect for liberal democratic values, to initiatives to establish new geopolitical "facts" in East Asian waters. Those suggest that the center of gravity for at least some conflicts is shifting away from military forces toward the political processes, thought leaders, and social media of the targeted populations. Rather than inciting a population to take a particular action, as the leak of the Zimmerman telegram did in accelerating the U.S. entry into World War I, campaigns today often seek to fragment citizen opinions and disrupt belief systems. The ultimate resilience of a nation or an alliance lies in the minds of its citizens who today are under persistent pressure.

There are many definitions of resilience, the best of which include proactive pre-crisis preparations and risk mitigation, effective incident management, and leveraging whatever shocks occur to build back better, as probability scholar Nassim Taleb advocates in his work, *Anti-Fragile: Things That Gain From Disorder.*[20] The Rockefeller Foundation defines resilience as:

> *The capacity of individuals, communities and systems to survive, adapt, and grow in the face of stress and shocks, and even transform when conditions require it. Building resilience is about making people, communities and systems better prepared to withstand catastrophic events—both natural and manmade—and able to bounce back more quickly and emerge stronger from these shocks and stresses.*[21]

The summary of resilience should therefore move from "bounce back" to "be prepared to bounce forward better."[22] How to strengthen the resilience of societies deserves more attention in conflict studies.

Cognitive-Emotional Conflict

Continued, long-term campaigns of disruption, perception management, and deception sow confusion and undercut values and convictions.[23] These campaigns are but one element of cognitive-emotional conflict. Many of their components are not new. They involve violence and the threat of violence, integrating kinetic and non-kinetic elements in ways that would be fully understood by Sun Tzu, Clausewitz, or John Boyd.

The American way of war historically has favored kinetic approaches in environments that clearly distinguish between combat and non-combat, where "one side distinctively wins while the other distinctively loses."[24] Violent action and its connection to policy have long been at the heart of Western military thought, but there also are complementary strategies. Sun Tzu did not clearly delineate between a state of peace and war, though violence and the threat of violence were part of his conception of statesmanship.[25] He did emphasize the importance of deception, perhaps since it helped the leader to "flow" between various states of conflict. Twentieth century military strategist John Boyd later addressed both the offensive and defensive sides of cognitive approaches, noting that strategy should "magnify and augment our inner spirit and strength" while swaying the uncommitted. It should also "isolate adversaries from their allies…[and from] one another, in order to magnify their internal friction, produce paralysis, bring about their collapse…so that they can no longer inhibit our vitality and growth."[26]

Information-based acts in cognitive conflict draw on many tools to "confuse, befuddle, discourage, confound, depress, deny, destroy, degrade, disrupt, usurp, corrupt, deter/dissuade, disconnect, cost-impose, dispose, convey weakness or worse, engender fear (or respect), herd/vector in desired direction and generally negatively impact on victims'/adversaries' ability to see, know, understand, command/control/access his own means, decide, act and be confident of his/her posture, processes or destiny…[These] actions will likely be applied around critical times."[27] Clearly they have been employed before in high-intensity wars (the deception operations surrounding Normandy), other armed conflicts (direct adversary messaging to populations during the Vietnam War and the First Intifada), and in measures short of armed conflict (propaganda and false news to undermine the legitimacy of governments or belief systems).

What is new today is the ease by which modern communications allow adversaries to bypass military forces, borders, and alliances to magnify their voices in the minds of our people, our adversaries, the uncommitted, and our allies.[28] Since experiencing disappointing results in Chechnya in the 1990s the Russians have been refining their "information-psychological" capabilities, which approximate the goals of netwar.[29] Parts of China's "three [unconventional] warfares" relate to efforts to implement "political work."[30] As future cyberspace activities evolve to destroy physical systems more effectively or disrupt essential services, they provide other ways to undercut the confidence of people in their governments.

There is an ample theoretical basis, and a range of operational capabilities, to support a portfolio of cognitive-emotional strategies, from offensive ones to influence opponents, to persuasive ones to encourage neutrality, to defensive ones to build cohesion. This is broader than a cognitive-emotional campaign in the military sense since key parts fall outside military control. Cognitive-emotional conflict is:

> *A struggle to affect the thoughts and values of people at all levels of an opponent's organization and society, using technical and other informational means, while preserving the resilience of one's own organizations and society, and attracting the uncommitted.*

Within this struggle of understanding an adversary's conscious and unconscious perceptions is the recognition that the process of creating actions to shape perceptions will be iterative. The next step is creating and highlighting mismatches in perceptions and using them as weaponized information to target the mind of the adversary and related populations.[31] Since it is impossible to understand perfectly how an adversary's perceptions can be shaped, messages will need to be tested continuously for effectiveness and adapted. Cognitive-emotional conflict thus extends across the entire continuum of conflict, as shown in Figure 2.

U.S. Advantages and Disadvantages in Cognitive-Emotional Conflict

Daunting as the military challenges may be, there are two greater problems: first, how to address coordination beyond the Department of Defense (DOD) in a whole-of-government framework? And then, how to move beyond government to achieve the kind of "whole-of-society" resilience that the nation, and its alliance partners, will need to face the coming cognitive-emotional challenges? The United States starts with a number of advantages, but also serious weaknesses.

U.S. Advantages in Cognitive-Emotional Conflict

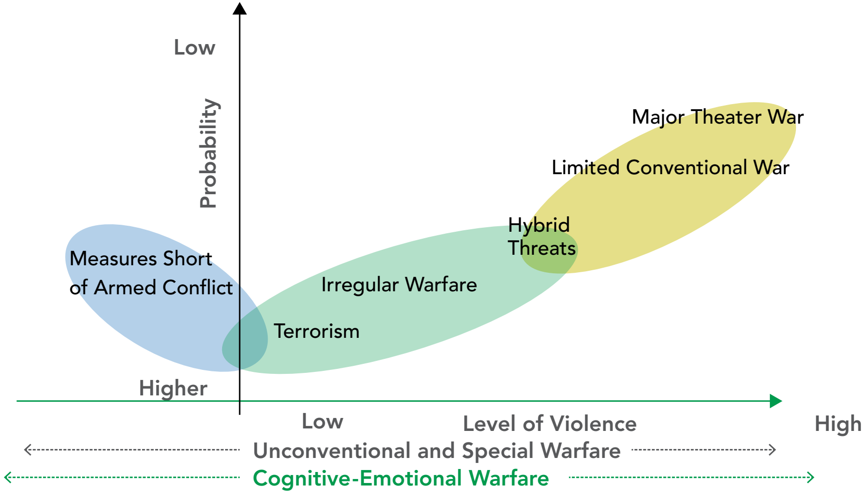
Military/Government Levels

DOD and the Intelligence Community (IC) have exceptional technical cyber capabilities across the full range of OCO, DCO, and CNE as well as many of the non-cyber disciplines, to include electronic warfare, operational deception, space, and command and control. Additionally, Special Operations Forces and parts of the cyber community can adapt quickly to emerging technology and changing circumstances. The U.S. hacking community also is more integrated into the cybersecurity community than in many other countries, partnering through programs like "bugs for bounty" and hackathons.

National Levels

Our diverse population and relatively open system is able to adapt in complex, uncertain environments. Many studies suggest that closed systems begin to lose their adaptability under adversity, and eventually come to be at risk of survival. Such closure can occur either through top down direction (such as isolating a national internet), or a self-selecting series of actions, such as choosing only reinforcing information sources (echo chambers) that limit understanding of a rapidly evolving environment.

FIGURE 2: Cognitive-Emotional Conflict Extends Across the Entire Continuum of Conflict.



Former Dean of Princeton's Woodrow Wilson School of Public and International Affairs, Anne Marie Slaughter, observed in 2009 that the United States ought to have significant advantages in a networked world that derive from the heterogeneity of its population, its geographic location, a horizontal social structure, and a culture of entrepreneurship and innovation.[32]

> *In a networked world, the United States has the potential to be the most connected country…If it pursues the right policies, the United States has the capacity and the cultural capital to reinvent itself.*

The United States possesses the checks and balances, diversity, and feedback loops, and is resilient enough to absorb lessons, learn from them, and adapt. A key is to recognize that "the antidote to netwar poison is active transparency," however painful and disruptive that may be to implement.[33]

U.S. Disadvantages in Cognitive Conflict

The exceptional increases anticipated in science and technology capabilities during the next 15 years will have social impacts as well as operational and strategic ones. Many technology fields such as biotech, robotics, information, nanotech, energy, and additive manufacturing are rapidly changing in parallel. These issues affect the winners and losers in society, the way nations interact, and the way our children think. They raise questions for policymakers, ambassadors, commanders, not just technical specialists. Technological changes, and their interactions, need to be considered as strategic variables in national security planning, but they rarely are today.[34]

Military/Government Levels

The United States and its allies, are not organized, trained, and equipped to be agile and effective in cognitive-emotional conflicts today.[35] U.S. military strengths and doctrine have been aligned more with conventional kinetic conflict than with nuanced cognitive-emotional approaches. Achieving integrated effects at strategic, operational, and even tactical levels is complicated by the way the U.S. now separates cyberspace operations, military information support operations (MISO), intelligence, civil affairs, and related fields into discrete disciplines with distinctive organizations, personnel systems, and operational concepts.[36] Though they often are intended to be mutually supporting, campaigns in each of these areas now may not interact as much as they should to produce integrated effects. Often they are executed at very different levels of classification by skilled operators who are doing their best, but who may be largely unaware of each other's needs and accomplishments.

The problem is compounded by how critical information flows increasingly are outside the government's control—for example, products of geographic information systems (GIS) from sources like commercial satellite imagery and unmanned systems—aerial, ground, and underwater. These are augmented by an explosion of new sensors, from smart phones to augmented reality devices, to the Internet of Things. Finally there is the volume, velocity, veracity, and value of information (IV4) produced by the 24/7 news cycle, amplified and accelerated by social media.

National Level

Most Americans do not recognize the threats posed by cognitive-emotional conflicts and weaponized information. Despite the nation's diversity, most Americans are poorly equipped, through language skills or cultural awareness, to engage deeply in foreign cultures.[37] This can make it hard to recognize that different nation states have different views of concepts such as soft power.[38] For example, Russia thinks of soft power as everything short of outright war (deception, fake news, etc.), while the United States often views soft power as something that attracts people to American ideals.[39] Such differences make it hard to project, or counter, narratives effectively in foreign environments; particularly given how the United States has cognitive-emotional conflict needs that extend globally, but few of our allies can execute cognitive campaigns beyond regional levels.

The United States thus far has given insufficient attention to crafting and disseminating compelling narratives that shape perceptions. We have allowed our once exceptional capabilities for cognitive-emotional conflict—e.g. in the information campaigns of World War II and the activities of organizations like the U.S. Information Agency during the Cold War—to atrophy, and we lack a consistent national narrative to tell our story. Additionally, U.S. practitioners are bound by asymmetric legal, moral, and ethical constraints that often keep them from being agile enough to compete effectively with skilled adversaries in the realm of social media. This admittedly is a complex problem for any open, democratic society that does not perceive an existential threat.[40]

Consider how Russia's state-owned news outlets routinely deliver government-sponsored messages that are increasingly being accepted as unbiased.[41] And al-Qaeda in Iraq did not need to match U.S. armor or firepower. It only needed to record improvised explosive device (IED) attacks for broadcast to the world. It is much easier to kill one American and broadcast the video to millions than it is to try to kill ten thousand Americans in a combined arms maneuver campaign. Effective cognitive-emotional conflict amplifies small events to create effects in the adversary's mind. Daesh has leveraged these techniques through social media and has broadened its appeal to new regions such as Southeast Asia much more rapidly than expected.[42]

U.S. practitioners of cognitive-emotional conflict need excellent situational awareness, supported by securely networked systems and processes with information flowing as freely as possible, even while trying to disrupt and isolate adversary equivalents. The stovepipes among U.S. tools for cognitive-emotional conflict may be understandable, but they cannot deliver integrated effects. Other nations have fewer artificial restrictions. For example, the Russians, like the Soviets before them, do not separate the intelligence, operations, and communications functions, but rather refer to a more integrated "radio-electronic struggle," which avoids many of the inefficiencies caused by divisions among personnel structures, doctrine, management, etc. These are part of whole-of-government approaches.

Improving the Odds of Success in Cognitive-Emotional Conflict

Some suggest that we are reaching the end of the post–World War II international security structure, pressured by the challenges of a risen China, the resurgence of Russia, worldwide migration, and terrorism, and the various national and transnational responses.[43] The emerging structure is not yet clear, but cognitive and emotional elements certainly will be part of any follow-on conflicts. This section addresses the military, whole-of government, and societal actions that could help prepare for cognitive-emotional conflict in our changing world.

Information as a Joint Warfare Function

In July 2017, Chairman of the Joint Chiefs of Staff, General Joseph F. Dunford, Jr., approved the designation of information as the seventh joint warfare function.[44] This designation of information as the seventh joint warfare function opens up possibilities for coordination that are just now beginning to be examined. A strategy for "Operations in the Information Environment" (OIE) was issued almost one year prior, so there is a basis for considering the closer integration of cyber and content along the full spectrum of doctrine, organization, training, material, logistics, personnel, and facilities—better known as DOTMLPF. Other information-based components that could benefit from closer integration include but are not limited to:

- strategic communications;
- electronic warfare, to include an electromagnetic pulse (EMP) attack;
- kinetic and non-kinetic operations;
- space and counter-space operations;
- operational security (OPSEC);
- military information support operations (MISO), a.k.a. PSYOPS;
- covert action/propaganda;
- controlled and uncontrolled leaks.[45]

These activities involve different skill sets, agencies, armed services, and even organizational cultures, and should include the Intelligence Community. Half steps are unlikely to be effective but, at the same time, trying to eat the whole elephant at once is likely to be overwhelming. First steps should focus on cross-cutting approaches to a few problems to maximize prospects for near-term successes. On the personnel side, recognize that not everyone will be able to perform well in this environment. Train and educate as broadly as possible, but focus on building a core team of exceptional practitioners.

Already the U.S. Navy has combined its intelligence (N2) and communications (N6) functions into an Information Warfare corps. Could/should similar functions be included by other armed services to improve integration and agility? Ironically, the potential split of U.S. Cyber Command from the National Security Agency may complicate these efforts to breakdown stovepipes.[46]

Alternatively, some have suggested that a new "Joint Concept for Cognitive-Emotional Warfare" be developed to give the idea of cognitive-emotional conflict a larger role in the training, budgetary, and force structure processes. Given the ongoing developments, this probably is premature. The other activities should be allowed to mature.

Reshaping the Broader U.S. Government for Cognitive-Emotional Conflict

The nation needs to convey, by all possible means, the narratives it seeks to represent it. Diplomacy—especially public diplomacy—is on the front line of this campaign, supported by aid programs, and the myriad of other messages the United States projects on a daily basis. Executive Branch departments other than Defense and State have important roles to play, as does industry.

The Department of Homeland Security (DHS), for example, is responsible for protecting the .gov domain and critical infrastructure. DHS has well-defined, whole-of-government management structures in-place for steady state and incident response activities.[47] These structures require collaboration with the private sector through mechanisms such as Information Sharing and Analysis Centers (ISACs) and Organizations (ISAOs), and response to a cyber incident could well be an important part of a cognitive conflict campaign.

Communications need to be aligned with strategy, which must be supported by both narrative and action.[48] Distorted information in a disinformation campaign can be reframed, refocusing can counter distraction, reaffirmation can offset dismissive efforts, and reassurance can address information intended to dismay.

Coordinating these activities is likely to be difficult, given the lack of an agreed U.S. national narrative at present, but it must be tried. Democracies have the added challenge of using information legally and ethically within severe constraints, which often are strained in cognitive-emotional conflict. Decisionmakers have no right to be wrong.

Increasing National Resilience against Cognitive-Emotional Conflict

Government action alone is unlikely to resolve key societal issues, given countervailing moral, legal, and ethical interpretations, as well as suspicions of the government in many quarters. For example, legal and privacy concerns are critical elements of a democratic society, and they need thorough vetting, even though this may impede rapid action on cybersecurity issues. Impassioned policy discussions over security and privacy have existed since the beginning of the internet, and doubtless will continue in new directions as technology continues to evolve. No one side has all the answers, but the debates are essential, and are a far better approach than top down unitary, directed solutions.

Singapore has postulated a "total defense" concept involving military, civil, economic, social, and psychological components.[49] It recognizes citizen participation as essential as connectivity increases and infrastructures become more interdependent. Signs like "our diversity is our strength" are omnipresent across Singapore. Not every nation can match the tight integration of Singapore's population and their general trust in government. However, as noted earlier, nations that have strong systems of checks and balances, feedback loops, and open information flows have great sources of resilience. These should be nurtured, for they are the basis by which the nation can absorb cognitive-emotional attacks and adjust, over time, to the cognitive-emotional campaigns against them.

At the same time, serious research is needed into the basis of, and limits to, societal resilience in a networked world, especially in democracies. For example, what will be the likely impacts on resilience of disruptions of services through cyberattacks on infrastructures? What differentiates a spirited divergence of views from unbridgeable divisions of worldview? In some cases, neuroscience may be able to provide insights.[50] As these are being worked out, the critical importance of transparency remains. The adjustments are not likely to be quick, smooth, or painless, but they must happen, and represent one of the nation's greatest strengths in cognitive-emotional conflict.

Parting Thoughts

Today's environment is particularly conducive to cognitive-emotional conflicts, owing to the rise of cyber interconnectedness and the range and reach of information sharing tools. There are billions of netizens and billions more will connect during the next few years. This level of connectedness accelerates change and can disrupt many of the policy formulation mechanisms that are legacies of the industrial age, "When decision-makers had time to study a specific issue and develop the necessary response or appropriate regulatory framework."[51] Cognitive-emotional conflict thrives in this dynamic, interconnected environment, and the "weaponization of information" is one way that it can challenge the established order. Actions, both violent and non-violent, can be tailored for nearly instant network dissemination. The nimble player who can shape perceptions generally wins against slow and methodical one.

Success in these sorts of contests requires the nimble, nuanced, and harmonized use, not only of all aspects of national power, but also of non-state and transnational instruments.[52] Strategy, narrative, and actions need to be aligned. Cyberspace operations need to be integrated with "other information-based attacks, defenses, or exploitations as a means for conveying influence, signaling, messaging, or executing strategic communications based on the information-based content itself."[53] All must be supported by intelligence attuned to each area. Decisionmakers and their staffs will need near-real-time situational awareness, yet with options that provide time for reflection. Parts of an engagement will proceed at machine speed with people "on-the-loop," rather than "in-the-loop," while other aspects will require nuanced cultural understanding, sophisticated narratives, and human contact.[54] Throughout, citizens must be informed in credible ways, amidst myriad countervailing information flows, many of them ill-informed at best, and malicious at worst. Conspiracy theories abound, amplified by information "echo chambers."[55] No organization today—government or civilian—is prepared to deal with all these forces effectively in real-time. PRISM

Notes

[1] This paper represents my personal views and does not reflect the opinions of National Defense University or the U.S. Government. It would not have been completed without major contributions by Maj Phillip Lere, USAF. Dr. Frank Hoffman, Dr. T.X. Hammes, and ADM William O. Studeman, USN (ret.), and Dr. Rebecca Goolsby provided invaluable insights. Any errors are my own.

[2] Cognitive processes involve the acquisition and understanding of knowledge which, while important, are not sufficient to address the full scope of emotions targeted by today's information and disinformation campaigns.

[3] Mark Laity, Director of Strategic Communications at NATO's Allied Command Operations (ACO) repeatedly made this point to a roundtable of senior Southeastern European (SEE) leaders on September 27, 2017.

[4] Cognitive-emotional conflict is defined later in this article. Information Operations are defined in U.S. Joint Publication (JP) 3–13 as "the integrated employment, during military operations, of IRCs [information related capabilities] in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own." JP–3-13, November 27, 2012 incorporating Change 1, November 20, 2014, ix. This definition makes it clear that IO primarily applies to military operations, although the "in concert with other lines of effort" could tie into "whole-of-government," or even "whole-of-society" conflicts. For more information see <http://dtic.mil/doctrine/new_pubs/jp3_13.pdf>. RAND notes IO and IW "… also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." For more information see <https://www.rand.org/topics/information-operations.html>.

[5] Resilience is defined later in this article.

[6] From the SMA description: "The Strategic Multi-Layer Assessment (SMA) provides planning support to Commands with complex operational imperatives requiring multi-agency, multi-disciplinary solutions that are NOT within core Service/Agency competency. Solutions and participants are sought across USG and beyond. SMA is accepted and synchronized by the Joint Staff/J-39 Deputy Director for Global Operations (DDGO) and executed by the Deputy Assistant Secretary of Defense (DASD) for Emerging Challenges and Prototyping (EC&P).

See, for example SMA Panel Discussion: Fake News Inoculation and Enhanced Population Resilience, a Department of State Perspective; Booklet July 6, 2017.

[7] Dr. Rebecca Goolsby proposes four "Rs" (reframe, refocus, reaffirm and reassure) to counter the four "D"s of disinformation campaigns (distort, distract, dismiss, dismay). Presentation to a roundtable of senior Southeastern European (SEE) leaders on September 26, 2017.

[8] F.G. Hoffman, Exploring a Continuum of Contemporary Conflict, December 2016, unpublished.

[9] Unconventional warfare (UW) is defined by U.S. doctrine as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow an occupying power or government by operating through or with an underground, auxiliary, and guerrilla force in a denied area." JP 3–14, *Unconventional Warfare*, September 2015. This mode of conflict is usually done covertly, with low signatures and limited footprint, and conducted primarily by Special Operations forces.

[10] Hoffman, working definition. In his formulation, "Measures Short of Armed Conflict" include so-called "gray zone" operations, which now are not clearly defined in doctrine. That said, others have provided working definitions of "gray zone activity" as "an adversary's purposeful use of single of multiple elements of power to achieve security objectives by way of activities that are typically ambiguous or cloud attribution, and exceed the threshold of ordinary competition, yet intentionally fall below the level of open warfare." U.S. Strategic Multi-Level Assessment (SMA) Gray Zone Effort Update, February 2017, 1. Special Operations Command (SOCOM) has used "Competition Short of Armed Conflict" (CSAC) in lieu of MSAC, ibid, 3.

[11] First established in the Joint Staff (J7) *Irregular Warfare Joint Operating Concept*, version 1.0, Washington D.C., September 11, 2007.

[12] Irregular Warfare often is abbreviated IW, which is confusing in the context of this paper with Information Warfare. Accordingly, "IW" in this paper only refers to Information Warfare.

[13] Hoffman, 19.

[14] Carl Von. Clausewitz, *On War*, translated by Michael Howard and Peter Paret, Princeton University Press,1976, 75. Sun Tsu *The Art of War*, translated by Lionel Giles, Amazon Classics, 2017, available at <https://www.amazon.com/Art-War-AmazonClassics-Sun-Tzu/dp/1542047528/ref=sr_1_3?s=books&ie=UTF8&qid=1502664791&sr=1-3&keywords=art+of+war>. This is a more nuanced formulation than what is sometimes translated as to "defeat an enemy without fighting is the acme of skill."

[15] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Volume 12, Number 2 (1993): 144¬46. Precise definition is used by Arquilla in his interview with FRONTLINE on March 4, 2003, available at < http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.

[16] Ibid,146.

[17] *Cyber Operations*, JP3–12(R), February 5, 2013,vii and I–3.

[18] Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense" DNI, 2012 available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2-3, et. seq.(emphasis supplied).

[19] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Vol 12, No 2 (1993), 144. Cited in Robert Brose. "Cyber War, Netwar, and the Future of Cyberdefense," 2012, available at <https://www.dni.gov/files/documents/atf/Cyber%20War%20Netwar%20and%20the%20Future%20of%20Cyberdefense_Header.pdf>, 2–3, et. seq.

[20] Nassim Taleb, *Anti-Fragile: Things That Gain from Disorder*, 2014, available at <https://www.amazon.com/dp/B0083DJWGO/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1>.

[21] Rockerfeller Foundation, "Valuing the Resilience Dividend: A New Way Forward," available at <https://www.rockefellerfoundation.org/our-work/topics/resilience/>.

[22] I am indebted to Dr. Dane Egli for his insights about this formulation.

[23] A speaker in Singapore recently referred to this as "slow burn" threats that erode public unity and confidence: Lin Qinghui briefing at the Asia-Pacific Programme for Senior Military Officers (APPSMO), Singapore, August 8, 2017.

[24] CAPT Phil Kapusta, USN, in SMA "Panel Discussion on the Gray Zone in support of USSOCOM," April 27, 2017, 4.

[25] Michael I. Handel, *Masters of War: Classical Strategic Thought*. London: Routledge, 3rd edition, 2000.

[26] Frans Osinga, Science, *Strategy and War: the Strategic Theory of John Boyd*. London: Routledge, 2007, 213.

[27] ADM William O. Studeman, USN (ret.) "Tutorial on Managing the Overlap Between and Alignment of Cyber, Information Warfare/Conflict/Operations and Intelligence (including all forms of security)," February 2017. Critical times include elections, preparation for military operations, during campaigns to build public support, etc.

[28] Osinga op. cit.

[29] Brose, op. cit., 10–11. The complement of "Information-Psychological" capabilities is "Information-Technical" efforts, which equate more to cyberwar.

[30] *Ibid*, 18–23.

[31] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," testimony before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017, available at <https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf>. Osinga, op. cit., 217.

[32] Anne-Marie Slaughter, "America's Edge: Power in the Networked Century," *Foreign Affairs*, January/February, 2009. Looking back, many aspects of this article now seem optimistic, but the points about the strengths the United States can derive from its diversity and networking seem valid.

[33] Brose, *op. cit.*, 28.

[34] James Kadtke and Linton Wells II, "Technology Is a Strategic National Security Component," *Signal* Magazine, January 2015, available at <http://www.afcea.org/content/?q=node/13831>.

[35] Linton Wells II, "Prepared for Battle, But Not Prepared for War," *Proceedings*, (U.S. Naval Institute Press: November 2017).

[36] Military information support operations— Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Also called MISO. (JP 3–13.2), available at <http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf>.

[37] This extends beyond inabilities to speak foreign languages or unfamiliarity with the norms of other cultures. Richard E. Nisbett, in *The Geography of Thought: How Asians and Westerners Think Differently...and Why*, 2004, examines differences in basic thought processes between US/European and East Asian societies. During a recent Compexity Workshop in Singapore, Dr. Cheong Siew An, in a presentation entitled "Complex Narratives and Identities," noted the difficulty in aligning cultural narratives with historical facts.

[38] Brose, *op. cit.*,15.

[39] Joseph S. Nye, Jr., *Soft Power: The Means To Success In World Politics*, New York: Public Affairs, 2009.

[40] See, for example, CAPT Wayne Porter, TEDx talk "A National Strategic Narrative & Role of American Communities." May 18, 2014, available at <https://www.youtube.com/watch?v=BWO8JJcqrVs>and the broader, website available at <http://nationalstrategicnarrative.org/>.

[41] See, for example: Peter Pomerantsev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*, Public Affairs, 2014; see also "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2014, available at <http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/>, accessed December 30, 2016.

[42] Jerard, "Índomitable Hydra," *op. cit.*

[43] Views expressed at Singapore's International Risk Assessment Horizon Scanning Symposium (IRAHSS), July 18–19, 2017.

[44] The U.S. military traditionally has recognized six warfare functions: Command and Control (C2), Intelligence, Fires, Movement and Maneuver, Protection, and Sustainment. A review of the National Military Strategy (NMS) this year led to an annex on "*Shaping the Joint Force*" that directed the joint force to "treat information as a joint function." Change 1 to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, dated July 12, 2017, established information as the seventh joint function, available at <http://dtic.mil/doctrine/new_pubs/jp1_ch1.pdf>.

[45] Studeman, *op. cit.*

[46] Patrick Tucker, "What the Announced NSA/Cyber Command Split Means," *Defense One*, August 18, 2017, available at <http://www.defenseone.com/technology/2017/08/what-announced-nsa-cyber-command-split-means/140362/>.Based on other reporting, it is not clear the NSA/Cyber Command split has been finalized.

[47] See, for example, Linton Wells II, Motohiro Tsuchiya, and Riley Repko, Improving Cybersecurity Cooperation between the Governments of the United States and Japan <https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf>, 4–9.

[48] Laity , *op. cit.*

[49] Lin Qinghui briefing at Asia-Pacific Programme for Senior Military Officers (APPSMO), *op. cit.*

[50] SMA, "Leveraging Neuroscience for Understanding the Cognitive Battlefeld," August 2017.

[51] These conflicts are shaped by diverse, dynamic forces, from accelerating technological change, to the Fourth Industrial Revolution as postulated by Dr. Klaus Schwab of the World Economic Forum in: Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond," January 14, 2016, available at <http://www.weforum.org/agenda/2016/01/>, accessed February 16, 2016. Many of these issues are beyond the scope of the Defense Department's role, but there are steps that DOD can take to help the nation deal with them.

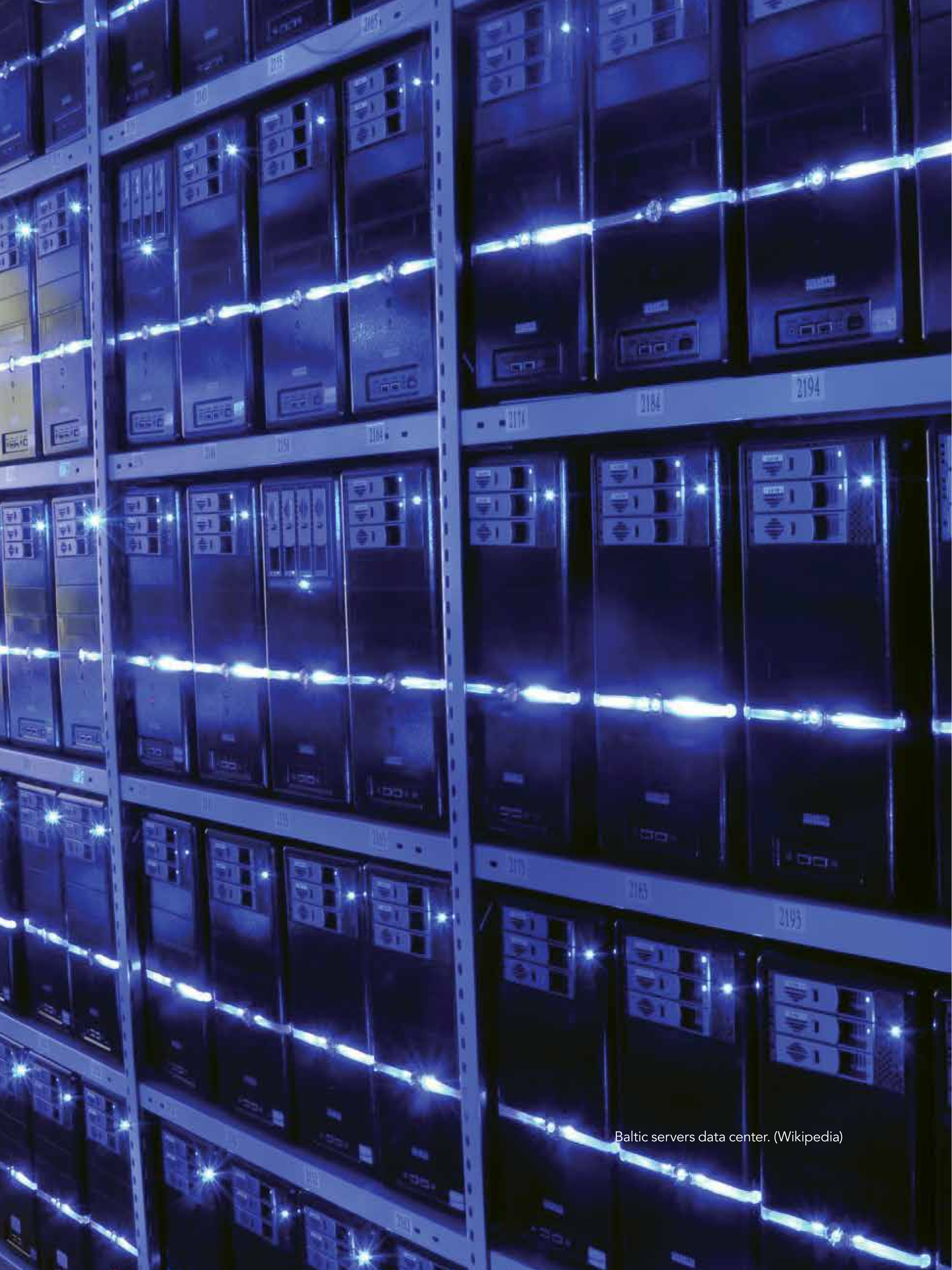
[52] The rapid spread of jihadist ideologies in Southeast Asia during 2015–17 shows an exceptionally nimble, nuanced and integrated use of non-state and trans-national instruments. See Jolene Jerard, "Indomitable Hydra: Transnational Terrorist Threat," presented at the Military Studies Programme Seminar 2017 at the S. Rajaratnam School of International Studies

(RSIS), Nanyang Technological University, Singapore, August 11, 2017.

[53] Studeman, *op. cit.*

[54] "Man-in-the-loop" refers to situations where people make the key decisions. "Man-on-the-loop" recognizes that some aspects of modern warfare, notable machine-to-machine computer operations move too quickly for people to be engaged at every step and so the person ON the loop must pre-delegate certain ranges of action to the autonomous subsystems when certain criteria are met. This is equivalent to delegating authority under "rules of engagement."

[55] Information flows that reinforce each other to support a particular point of view, or world view, form an "echo chamber."



Baltic servers data center. (Wikipedia)

How is NATO Meeting the Challenge of Cyberspace?

By Jamie Shea

Historians of international relations are familiar with the hinge-year concept when trends that previously had been largely subterranean suddenly crystallize into a clear and immediate danger, forcing policymakers to wake up and take action. When it comes to cyberspace, the past year has certainly smashed any complacency about our ability to anticipate and counter the growing sophistication of cyberattacks. As fast as we have tried to catch up, the speed and global impact of these attacks continue to outrun us. 2016 witnessed the first major attack via the Internet of Things when a DynCorp server in the United States was hacked through video surveillance cameras. We also saw the first attacks driven by artificial intelligence, and increasing evidence of collusion between state intelligence services and organized crime networks.

Yet it is not the much discussed theme of the economic damage inflicted by cyber crime in the past year that has dominated the debate. It is more the use of cyber as an instrument of state policy, political influence, and manipulation. From being a useful tool of espionage and intellectual property theft, cyber intrusions have evolved into a potent instrument of hybrid warfare and outright political vandalism. Ukraine, for example, has been the victim of an unprecedented and systematic campaign of cyber bullying. It has acknowledged up to 2,000 orchestrated cyberattacks since Russia occupied Crimea in March 2014. It has suffered disruption to its election voting system, train and airline on-line booking, ports, electricity grid, and most recently, the massive elimination of tax and financial accounting data through the NotPetya malware. Initially disguised as a ransomware attack similar to the previous WannaCry, a hack that affected more than 200,000 computer networks in 150 countries, it soon became clear that the data encrypted was being destroyed, and that the motive of the attack was not financial gain but rather economic and structural sabotage. Although companies in other countries were also affected by NotPetya, 80 percent of the impact was in Ukraine.[1] Intelligence analysts now agree that NotPetya was a state-driven effort. All of these orchestrated cyber campaigns suggest that Ukraine is being used as a laboratory or proving ground to test a range of cyber weapons and assess their impact, with widespread collateral damage elsewhere accepted as a consequence of doing business; or even as a way to cover tracks.[2]

Given the difficulty of technical attribution and the inability of governments to deter or retaliate against cyberattacks in a manner that demands the attacker's attention but avoids unwanted escalation, NATO has

Dr. Jamie Shea is Deputy Assistant Secretary General for Emerging Security Challenges at NATO. The views expressed are entirely those of the author and should not be construed as an official position of NATO.

had to take a hard look at its preparedness, not only to fend off cyberattacks but also to preserve its political and military freedom of navigation in the cyber domain. The revelation in a recent *Washington Post* article of how the Obama Administration rejected nearly all proposed responses to Russian incursions into the communications of the Democratic National Committee because they were deemed to be ineffective, escalatory, or would compromise long-term U.S. intelligence gathering and prematurely expose U.S. offensive cyber capabilities, caught NATO's attention.[3] There is growing awareness that Russian operational activity built around groups such as APT28 is aimed at inflicting damage to the reputation and cohesiveness of organizations such as NATO.[4] Consequently, reducing the strategic cyber threat to the functionality of governments and societies and making cyberspace more stable and transparent has become as important to international peace and order as nuclear arms control or the conventional balance of power.

The starting point for this effort is the recognition that every future crisis or conflict will have a cyber dimension, and that just as NATO has had to build missile defense and conventional postures into its traditional nuclear-based deterrence strategy, it will need increasingly to incorporate cyber expertise and capabilities as well. This will require not only planning and resources but an important intellectual effort to better understand the precise contribution that cyber capabilities can make to deterrence and defense or indeed crisis resolution, and when military commanders might want to use them in preference to traditional military tools.

Key questions include; is it worth investing more in cyber efforts than conventional equipment in terms of cost-effectiveness? When does it make more sense to invest scarce resources in people skills or better processes rather than upgrading technology? Can the collateral damage of cyber effects be precisely assessed and contained? Will their impact be short-term or long-term, tactical or strategic on the battlefield? Can cyber capabilities be incorporated into existing NATO command and control structures, or do they require more distinct and specialized structures?[5] Most importantly, how can senior Alliance political and military leadership train itself to be as efficient in assessing and responding to a hybrid operation based on cyber as to a crisis involving political, economic, conventional, or nuclear elements; or in the more traditional domains of land, sea, and air?

Many key aspects of cyber crisis management will need to be explored in this discussion: the use of exercises; what kind of intelligence/attribution picture is required; what kind of force generation of cyber effects as part of a broader spectrum of crisis response measures; and how to do cyber messaging to enhance deterrence as well as public support and legitimacy for NATO's actions, especially in an environment where cyber capabilities are shrouded in considerably more secrecy than the usual elements of the diplomatic and military toolbox. In the course of this discussion, it has also become clear that it is difficult to determine appropriate messaging on cyber activity, particularly when it comes to the timing, scope, and utility of offensive options, and that the best approach continues to be to learn the lessons from past attacks and improve defenses.

Developing the Toolbox

The sense of alarm regarding the evolving cyber threat to Allied nations as well as to NATO itself should not detract from the steps that the Alliance has already taken toward being a more cyber-capable and enabled organization. At the very least, these have considerably enhanced NATO's cyber literacy and defined a framework to take cyber work forward with more systematic political guidance and oversight. NATO declared at its July 2016 Summit in Warsaw, that the Alliance now considers cyberspace as a fifth operational domain (in addition to land, sea, air, and space). This essentially took NATO from the protection of the internal network (information assurance) to the cyber defense of every military activity (mission assurance).

In order to adjust to this new reality in which cyberspace is not only a new fifth domain of warfare in its own right, but also impacts the four traditional domains of warfare, NATO defense ministers in February 2017 approved a roadmap outlining the steps needed for the Alliance to fully implement the domain concept by 2019. This roadmap provides for a closer relationship between the Supreme Allied Commander Europe (SACEUR) and his Allied Command Operations, and the NATO Communications and Information Agency in The Hague, which is responsible for the daily protection and monitoring of NATO's networks in peacetime, and for the security and acquisition of NATO's information technology. This will ensure a smooth transition from civilian to military responsibility in a crisis situation. NATO is also updating its operational plans to better incorporate and prioritize cyber defense and to have a clearer sense of related requirements during operations.

Clearly, cyberspace has accelerated the speed at which crises can unfold, leading to the requirement for much better and earlier situational awareness and responsive decision-making. Operating "at the speed of relevance" has become the new buzz phrase. Accordingly, NATO's military commanders are working on a set of crisis response measures that will allow them to initiate forward scanning of networks, active defense measures, and the activation of a back-up NATO Computer Incident Response Capability (NCIRC). At the same time, a real effort must be made to understand how NATO's potential adversaries (Russia for example) are conceptualizing cyber in their doctrine, and what lessons they are learning from their ongoing covert cyber operations to develop this doctrine and adapt their cyber capabilities to a spectrum of projected missions. If we cannot stand still, then we must assume that they are not standing still either.

As NATO moves toward cyberspace as a domain, it needs to practice better to cope with offensive cyber as part of an access and area denial strategy, and rehearse more realistically these scenarios in its crisis management exercises and also in its Trident series of military exercises. This means better aligning cyber work with the Alliance's enhanced forward presence in Poland and the Baltic States, and its associated graduated response plans, particularly when it comes to SACEUR's ability to exercise full control of his area of responsibility and get reinforcements into place quickly. It also means a better coordination of effort across the NATO Command structure. Already SACEUR has set up a Cyber Division at Allied Command Operations, in order to better identify requirements and ensure that NATO's capability packages to common fund its acquisitions reflect the cyber dimension.

In this respect, NATO will need to meet the challenge of accelerating its upgrades to its information technology and to the NCIRC. NATO must move from a culture where capabilities are acquired in big chunks or platforms and at intervals of ten or fifteen years, to one in which information technology can be constantly upgraded in an evolutionary way, with incremental investments on a more frequent basis. The analogy is not going from an old car to a new one but constantly modifying the car so that it becomes impossible to determine when the old car has disappeared and the new one has taken its place. Otherwise there is a danger of technology becoming obsolete every two to three years, and that NATO's acquisitions process will constantly leave NATO behind the technological curve. If NATO's current capability packages are overloaded with too many different elements, and take an average of 16 years to implement, this challenge will not be met. Clearly, to improve on cyber delivery, political guidance, which is next due in

June 2019, has to be much more expansive and detailed on operational cyber requirements and capabilities than we have seen in the past.

Finally, another requirement associated with making cyberspace an operational domain is that NATO will need to learn more from its Allies who have already moved in this direction, such as the United States, the United Kingdom, France, and the Netherlands; how their models are working, and how they are intending to use cyber effects as part of their military operations. Some Allies, like Estonia and France, are putting the emphasis on a reservist force of civilian cyber specialists and cyber as a fourth army with a light, agile structure rather than as part of a classic, top heavy military chain of command. Should cyber follow a similar model in NATO at a time when the Alliance is refashioning its command structure to support corps level, heavy armoured and combined arms operations in Eastern Europe? NATO's political guidance for these issues is all the more important as NATO will not develop offensive cyber capabilities and would therefore need to rely upon national capabilities (subject to political approval by NATO overall) in instances where NATO military commanders believe that a cyber effect rather than the use of a conventional weapon is the best way of producing a desired military outcome. The U.K. Defense Minister has already offered U.K. national cyber capabilities to NATO on a voluntary basis, and other Allies may well make similar commitments in the near future. In the meantime, NATO's Cyber Defence Committee will work on a set of agreed principles for how a mechanism could function within NATO to give Allies effective political oversight for these national contributions used in the collective name of the Alliance. A question is whether these national cyber contributions could be used in a pre-conflict, hybrid warfare scenario, or only once a full-scale kinetic conflict has broken out.

The success of cyber as a domain ultimately depends on a two-way process. NATO must optimize the ability of cyber instruments to support classic military operations on land, sea, or in the air, but also ensure that the future NATO organizational construct and command structure have the requisite skilled personnel, rules of engagement, operational planning, and rapid access to capabilities to support advanced cyber operations. Additionally, as the Alliance deploys advanced capabilities, such as Global Hawk observation drones, joint intelligence surveillance and reconnaissance sensors, integrated air and missile defense, and its new air command and control system, these will need to be hard proofed against cyberattacks. Therefore, cybersecurity needs to be factored into all acquisition programs and in the systems design and development, rather than as an afterthought.

Cybersecurity needs to be factored into all acquisition programs and in the systems design and development, rather than as an afterthought.

The Cyber Defense Pledge

The second major initiative of NATO's 2016 Warsaw Summit was to adopt a Cyber Defence Pledge. Readers of this article will be familiar with an earlier Pledge from NATO's previous Summit in Wales in 2014 for each Ally to spend a minimum of 2 percent of its GDP on defense. The Cyber Defence Pledge commits Allies to spend at least a portion of this extra investment on improving national cyber defenses, even if there is no specified minimum amount. Effective cyber defense depends upon building a community of trust in which there are no weak links in the chain.

Otherwise, the more cyber capable Allies might be reluctant to share sensitive information and expertise with Allies who have not brought their national cyber defenses up to a minimum level of security. As NATO depends in nearly every area on national capabilities rather than commonly owned assets (AWACS aircraft being the exception), its ability to operate in the cyber domain depends upon its success in setting more ambitious capability targets for its member states, and to encourage them to plug identified gaps. By inducing the Allies to perform more regular assessments of their levels of preparedness, the Cyber Defence Pledge should make this effort easier in the future.

Allies have carried out self-assessments of cyber defense hygiene by reporting on seven capability areas—from strategy, organization, processes and procedures, threat intelligence, and partnerships, to capabilities, and investments. They have been asked to benchmark these assessments on a scale from advanced to relative beginner. National responses will allow the NATO staff to develop more precise and relevant metrics, as well as to form a more reliable common baseline of overall NATO capabilities. In turn, this greater transparency will help the NATO staff to identify gaps and prioritize requirements. On this basis, the well-known NATO Defence Planning Process, which has already incorporated a set of basic cyber capability targets for each NATO member state, will be able to suggest more ambitious targets better adapted to the needs of individual states in the future. The peer pressure that greater transparency should generate will incentivize Allies to meet their assigned targets and to stimulate bilateral assistance. An initial report on the first stage of the Cyber Defence Pledge was provided to NATO Defence Ministers last June. The good news is that for the 2017–19 cycle, all the capability targets set by NATO's Defence Planning Process have been apportioned and accepted by the Allies—for the first time, it must be said.

Building a True Cyber Defense Community

Beyond these two flagship initiatives of the 2016 Warsaw Summit, a good portion of NATO's effort to step up its game in cyber defense, is to enhance its ability as a platform to assist the Allies across a whole spectrum of cyber defense needs. For instance, a new memorandum of understanding (MOU) between NATO Headquarters (HQ) and individual Allies has been offered to improve intelligence sharing, crisis management, and lessons learned from cyberattacks. Already 22 of the 29 Allies have signed this new MOU. NATO has established a new intelligence division with a strong cyber threat intelligence function, which should incentivize Allies to provide more early warning and advance notice of cyberattacks or malware and not only lessons learned and post–incident information. Enhanced intelligence sharing among Allies will not only help to parry cyberattacks or to limit their damage but also to build over time a much more detailed and comprehensive picture of hacker groups, proxies, methodologies, and attribution techniques.[6]

One of NATO's most useful contributions to its member states is in the organization of trainings and exercises to improve the skill set not only of the 200 operators in the NCIRC and the NATO command structure, but also those of national cyber defense teams. The annual *Cyber Coalition* exercise now attracts more than seven hundred participants, and the *Locked Shields* exercise, involving 900 participants this year and won by the Czech Republic, is recognized as one of the most demanding and intensive Red Team–Blue Team exercises. This year it exercised the cyber vulnerabilities of drones, power grids, and programmable logic controllers. A strategic storyline was used to put the technical exercises in a contemporary political context. Both of these exercises take place at the NATO Cooperative Cyber Defence Centre of Excellence in Estonia and have

Operation *Locked Shields 2017* arranged by the NATO Cooperative Defence Center for Excellence. (NATO Cooperative Defence Center for Excellence) the use of the recently upgraded cyber defense range, which Estonia has offered to NATO.

Beyond exercising, NATO must train civilian and military personnel on a regular basis in cyber defense concepts and basic procedures, as well as organize courses on cyber hygiene for end-users across the entire NATO enterprise. A cyber security scorecard developed by the United States can help to visualize and manage basic cyber hygiene in real-time, focusing on the protection of sensitive data, information management, and cryptology.[7] Portugal has taken the lead in the Alliance on this type of training and education and will soon acquire the NATO Communications and Information School, which is being transferred from Italy to Portugal. The plan is to augment this school with a Cyber Defence Academy, which will both serve as a training center as well as a forum for a permanent interchange among NATO personnel, academia, and industry, with a cyber laboratory to facilitate innovation and experimentation. At the same time, NATO is assisting those Allies who have agreed to lead smart defense projects in cyber defense. In addition to Portugal's project on education and training, Belgium has successfully led a group that has developed a malware information sharing platform, which has not only been implemented among Allies but also between NATO and the European Union. A variant of this is also being used to facilitate the exchange of information between NATO and industry, with the possibility of more open as well as more confidential platforms according to the level of certified access and the sensitivity of the information being shared. A third cyber defense project focuses on situational awareness and incident coordination, including an operations and maintenance contract. The system has been successfully implemented by the Netherlands and Romania. All in all, 25 Allies and six Partners participate in smart defense projects.

Moreover, NATO now has a Cyber Defence Committee. This has been instrumental in persuading Allies to send cyber experts to NATO HQ on a permanent basis and to improve links between HQ and important national centers, such as Cyber Command and the National Security Agency in the United States, or its counterpart, the Government Communications Headquarters (GCHQ) in the United Kingdom. The Committee also serves as a focal point for industry and the NATO military command structure and NATO agencies to provide inputs into the policymaking and decisionmaking levels of NATO. New models for priority items like advanced technical measures, cyber resilience and robustness constructs, risk management models, and cyber security standards can be presented and validated by the Committee, which also has responsibility for monitoring NATO's Cyber Defence Action Plan implementation, updating the overall policy, and reporting in detail on progress to every meeting of NATO Defence Ministers. The Committee is the essential link between the technical operating level and the policymaking level, without which progress would be ad hoc and uncoordinated. A Cyber Defence Management Board within NATO HQ brings all the relevant actors together to assess and respond to specific cyberattacks and other incidents and to regularly monitor threat intelligence and early warning indicators. All these various activities are helping to make NATO the natural platform for setting the level of ambition and defining a common set of standards and requirements for its member states in cyber defense.

It Takes a Network to Defeat a Network

Finally, if NATO is to raise its game, it must have even stronger partnerships. Collaboration is the mantra in the cyber domain. Successful cyber defense depends upon being able to bring a much larger cast of actors around the same table than in the past, when we were dealing with much more limited and largely uniform circles to handle things like nuclear deterrence or missile defense. Yet collaboration even if necessary is not automatic. It requires full-time attention and resources to create and sustain relationships, as well as incentives so that over time partners believe they are getting as much out of the relationship as they are being asked to put in. Partnership should not become an end in itself, with networking for the sake of networking. Resources are limited so decisions must be made regarding which partners have to be prioritized and in which stages. Moreover, every organization must determine how many of its essential functions it needs to provide in-house and which ones it cannot manage by itself and can more cost-effectively outsource to outside entities. In sum, partnership needs as much of a strategic approach as any other aspect of cyber defense and must be driven from the top.

Toward this purpose, NATO has reached out to industry and formed a NATO Industry Cyber Partnership. Thus far, the NATO Communications and Information Agency has concluded twelve individual partnership arrangements with industry to share threat intelligence and early warning indicators. This has proved its worth in facilitating real-time information-sharing and rapid assessment of the recent WannaCry and NotPetya attacks. An improved series of NATO industry workshops, such as the annual NATO Information Assurance Symposium in Belgium and a series of threat vector workshops, are bringing industry and NATO together to discuss innovation, improving procurement and acquisition, and threat intelligence. Another area of interest for NATO is industry's experience of resource prioritization: when is it best to spend limited budgets on personnel and skills vis-à-vis technology upgrades or improved processes? This engagement with industry is also designed to help NATO better understand which security products are out there on the market which NATO could better exploit while also helping industry to see where NATO's procurement is likely to be heading in the future. A key concept of innovation is "fail fast," as effective cyber defense would be hampered if it takes too long to determine which innovative products will work and which will ultimately under-perform.

The NATO Industry Cyber Partnership can also improve supply chain management and stimulate diversity on the supply side. An information exchange has been set up at the NATO Communications and Information Agency that has been conducting pilot projects to see how we can better link up with academic research and small and medium-sized companies that are often in the forefront of innovation but which have often been reluctant to engage NATO directly or uncertain where to plug in to the NATO bureaucracy.[8] Hopefully, in time this innovation exchange will benefit from NATO common funding to organize trials, demonstrations, and simulations of NATO networks to test the usefulness of various products in a real-time environment. At all events, Allies are now sharing more information on their trusted industries, making it easier for an Ally in one country experiencing a cyber disruption, for instance on a power station or water facility, to identify in another NATO country a company that has the expertise to offer a rapid response with certified technology and supply chain security.

At the same time, NATO is building stronger relationships with other countries that have concluded a formal partnership arrangement with the Alliance. A political framework arrangement on cyber defense was recently agreed with Finland. A trust fund for the provision of cyber defense equipment and analytical and forensic capabilities is in operation with Ukraine. Moreover, NATO has been helping countries such as Jordan, Moldova, and Georgia with cyber defense organization at the national level, doctrine, and training. Partners are increasingly joining the Cooperative Cyber Defence Centre of Excellence in Tallinn (Sweden being the latest) or sending staff or observers there. In Brussels, NATO and the European Union (EU) are now coming together more closely in the cyber defense field. A technical arrangement on the sharing of non-classified information between NCIRC and the EU Computer Emergency Response Team (CERT–EU), which certifies that a company has fulfilled the legislative criteria required in each country, has been in operation for more than a year. The recent action plan to implement the NATO–EU Joint Declaration provides for more NATO–EU interaction; for instance in sharing information on operational planning for cyber defense during military missions, harmonizing training requirements, cooperating more on research and development, and standards between the European Defence Agency and NATO's Allied Command Transformation, and more mutual participation in each other's training and exercises, such as NATO's CMX, Cyber Coalition, and the EU's Cyber Europe. The current Estonian presidency of the EU has made information technology security its top priority. This should help NATO and the EU to hold more table top exercises and do joint strategic thinking on the future of the internet and how to promote better governance and norms for cyberspace, particularly at a time when the GGE (Group of Governmental Experts) process in the United Nations has stalled.

Whereas we have a good idea how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyberattacks, even when they are clearly designed to undermine our governments or our political processes.

Working at the Top but also at the Bottom

Cyber differs from the other domains of conflict: the pace of innovation is much faster, the technology is much more decentralized, and many more actors are involved, for better and for worse. Resources must be spread over a far greater number of functions and applied much more selectively than in a conventional capability program if a cyber construct is to operate successfully. Many more countries, groups, and levels of threat and risk have to be monitored and assessed simultaneously than is the case with classic conventional or nuclear adversaries. There is the problem of attribution and as the recent hacking during the U.S. elections has shown, still a good deal of uncertainty as to when a cyberattack, which does not necessarily kill people or destroy anything physical, can really be considered an act of aggression justifying retaliation. Whereas we have a good idea how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyberattacks, even when they are clearly designed to undermine our governments or our political processes. We can try to privately warn the suspected perpetrators; we can impose sanctions or indict certain individuals or organizations, as the United States has done in response to the Yahoo attack and the 2016 election interference; but as long as an adversary judges the gains to significantly outweigh the risks, then deterrence is not going to work.[9] So we will have to think more strategically about increasing the penalties and limiting the gains as we go forward. At the same time, cyber is problematic because as we contemplate the more strategic use of cyber, we still have to deal with the more conventional problems we have been confronting for the past 20 years or so.

In the first quarter of 2016, there was a 250 percent increase in the number of phishing sites and related email traffic vis-à-vis the final quarter of 2015.[10] The most recent McAfee Labs threats report warns that for every ten phishing emails sent by attackers, at least one will be successful. McAfee presented ten real emails to more than 19,000 people from across the globe and asked them to identify whether they were dangerous or legitimate. It found that 80 percent incorrectly identified at least one phishing email.[11] According to Verizon, 30 percent of phishing messages are opened and around 12 percent allow the attack to succeed by clicking the malicious attachment or link.[12] In 2016, there was a 400 percent spike in ransomware families with 15 new ones discovered on average every month.[13] Meanwhile, denial-of-service attacks are becoming larger and the average pay out from business email compromises is now running at $140,000.[14] These examples demonstrate that as we grapple with the new threats and challenges, we are still struggling to get the basics right, and are still vulnerable to the oldest and simplest intrusion techniques.

Accordingly, the cyber domain will require NATO to increasingly work top down on anticipating the strategic trends and adjusting policy and doctrine more quickly, while working bottom up at improving basic cyber hygiene to lower its attack surface and reduce the scope for own goals due to basic human error. What was after all so depressing about the manipulation of the U.S. elections was the fact that so much damage could be inflicted through the simple expedient of a miscommunication between a senior Clinton campaign official, John Podesta, and an IT specialist regarding whether a suspicious email was real or fake. There is a lesson here for all of us; that we will never have effective cyber defense if we raise our own game but fail to raise that of all of our colleagues and partners across the whole enterprise at the same time. Often policymaking falls into periods of decision and periods of implementation, but in reality we need to learn better to do these things simultaneously—learning to transform the plane while we are flying it—if we are to keep pace, let alone ultimately master the evolving cyber threat. PRISM

Notes

[1] For instance, the Danish shipping company Maersk had its container traffic paralyzed around the world losing US$300 million and one UK company, Reckitt Benckiser, suffered £120 million in losses.

[2] For instance, Russia has used WannaCry and NotPetya to claim that it is also the victim of cyberattacks, as some of its own ministries and companies such as Rosneft have been impacted.

[3] Greg Miller, Ellen Nakashima, and Adam Entopus, "Obama's Secret Struggle to Punish Russia for Putin's Election Assault," *Washington Post*, June 23, 2017.

[4] Matt Burgess, "Exposed: how one of Russia's most sophisticated hacking groups operates," *Wired*, January 11, 2017.

[5] France, for instance, has established the post of ComCyber to the Minister of Defense.

[6] A closer relationship with the EU's Europol agency and its Cyber Crime Centre would be useful here, given Europol's database on criminal forensics.

[7] United States Department of Defense, "Improving Cyber Basics—DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard," December 2016. Available at < http://dodcio.defense.gov/Portals/0/Documents/Cyber/CNDSP%20Plain%20Language%20Overview%20-%20DISTRO.pdf?ver=2017-01-31-125734-897>.

[8] In Europe, 70 percent of the market.

[9] United States Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017.

[10] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report: 1st Quarter 2016," May 23, 2016.

[11] McAfee Press Release, "97% of People Globally Unable to Correctly Identify Phishing Emails," May 12, 2015.

[12] Verizon, *Data Breach Investigations Report*, 2016.

[13] Trend Micro, *The Next Tier - Trend Micro Security Predictions for 2017*, December 2016.

[14] Ibid.

Photos

Page 18: Balic servers data center. From Wikipedia, available at <https://fr.wikipedia.org/wiki/Fichier:BalticServers_data_center.jpg>. Licensed under Creative Commons Attribution-Share Alike 3.0 <https://creativecommons.org/licenses/by-sa/3.0/>. Photo unaltered.

A guided-missile destroyer conducts replenishment operations with a dry cargo and ammunition ship in the Pacific Ocean. (U.S. Navy/Jeremy Graham)

Power Projection in the Digital Age

The Only Winning Move is to Play

By Darren McDew

Logistics is the lifeblood of the Joint Force. It requires an effective distribution network as its heart, moving and sustaining the force at the right place and at the right time—all the time. U.S. Transportation Command (USTRANSCOM) delivers that decisive force, projecting American power globally through the robust Joint Deployment and Distribution Enterprise (JDDE) and leveraging the expertise of more than 140,000 professionals. No other nation in the world can compete with the United States in conventional warfare because we plan, secure, and distribute combat capability so well. As a result, many military planners are now value-programmed to believe that a soldier or bullet will always be where it needs to be, when it needs to be there—on demand.

Established in 1987 to enable wartime transportation, USTRANSCOM now manages the continuous delivery of cargo and personnel in conflict and in peace. With a worldwide mission and ever-changing requirements, USTRANSCOM's success hinges on far more than sufficient ports, planes, ships, and trains. In this digital age, USTRANSCOM is completely dependent on the cyber domain to oversee, plan, and synchronize operations across the entire JDDE. This digital dependence incurs risk.

Our adversaries are keenly aware of this uniquely American strength and are pursuing advantages to undermine it, namely by disrupting our ability to operate in and through cyberspace. As our adversaries evolve their capabilities to exploit the cyber domain, we in turn must change the way we think about operating in the digital space. However, unlike the 1983 movie "War Games," which concluded the only winning move in thermonuclear war is not to play, we cannot afford failure in cyberspace—we *have* to play.

The Changing Battlespace

On February 8, 1904, Japan launched a surprise attack on the Russian-held Port Arthur on the Korean Peninsula, a critical logistics asset to Russia as a warm water harbor for their Pacific fleet. Russia responded with deployments along both a 5,500 mile Trans-Siberian railway and an epic sea journey by their Baltic fleet. However, Russia simply could not muster the combat power to aggregate forces against Japan in a

General Darren W. McDew, USAF, is the Commander of U.S. Transportation Command, one of nine Unified Commands under the Department of Defense. USTRANSCOM is a global combatant command with functional responsibilities for air, land, and sea transportation for the Department of Defense, ultimately delivering national objectives on behalf of the President and Secretary of Defense.

realistic time period. The rail line was single-track and non-continuous, requiring the trans-loading of all cargo from railcars to ships and back to railcars to cross Lake Baikal. The Baltic fleet sailed more than 20,000 miles from Europe and around Africa to find themselves with depleted supplies and lacking support against a superior Japanese naval fleet. After fighting through the night, Russia's Baltic fleet ceased to exist. With challenged and constrained lines of communication, Russia could not mobilize or sustain its military, and Japan forced it to negotiate. Today, our lines of communication exist as much in cyberspace as they do across rail and sea.

History demonstrates the pivotal role logistics plays in the success of a military campaign and how irrelevant the best laid plans become when a force cannot rapidly deploy or sustain itself. If we consider the changing battlespace from a historical perspective, it becomes instantly apparent that we cannot afford a deployment failure and that we must appreciate the vulnerabilities created by operating in cyberspace.

For the United States, the lesson is demonstrative—without USTRANSCOM's engaged cyberspace presence, an adversary could disrupt or deny movement within our distribution network and compromise or corrupt sensitive information. Without a corresponding cybersecurity focus to complement our developing physical capabilities, adversaries will augment their conventional forces with robust and practiced digital disruption skills to target our softer delivery support systems. This disruption may transcend USTRANSCOM's ability to deny, deter, or defeat, placing the nation's strategic objectives at greater risk. Logistics readiness is wartime readiness, and that means we need to guarantee superiority in the cyber domain to survive and operate effectively in the more traditional domains.

Logistics readiness is wartime readiness, and that means we need to guarantee superiority in the cyber domain to survive and operate effectively in the more traditional domains.

Current events show just how disruptive the cyber threat can be—leaked personal information, compromised email registrations, hacked financial databases, and massive denials of service or access. Each event further pushes conflict outside more conventional designations like peace or war. We must be emboldened to transform how we wage war in this new context, and that starts by redefining the changing battlespace. Specifically, the growing impact of the cyber domain permeates across parochial understandings of air, land, maritime, and space. Blurring the lines between these domains results in a gray zone where hostile actors can operate with limited attribution and with relative impunity.

Further complicating the gray zone is adversarial engagements in the digital space. Commercial industry represents roughly 50 percent of USTRANSCOM's wartime transportation capability, and nearly 90 percent of our traffic flows on unclassified networks to and from our commercial providers. USTRANSCOM operates in this cyber gap between our military and industry networks, spanning the jurisdictions of the Department of Defense (DOD) and the Department of Homeland Security (DHS). If we do not address this communication seam that exists between DOD and DHS, we leave U.S. military logistics susceptible to an inability to rapidly aggregate combat power. Much like Russia struggled a century ago in protecting the timely delivery of their capabilities, we will be at risk of cyberattack or a cyber-enabled strike against air, land, sea, or space movements.

Physical control of the global commons is no longer enough to assure our ability to project power through increasingly contested distribution networks. We require a robust cyber posture as the foundation to protect ourselves from an adversary capable of achieving strategic objectives without ever using kinetic force. An adversary no longer needs to attack physical lines of communication to blunt American power. Instead, the adversary only needs to deny our ability to move the force by attacking our virtual lines of communication or injecting doubt into the system, causing us to question our operations or the integrity of our deployment data. Understanding the changing nature of war, our challenge is maintaining mission assurance in a cyber-degraded environment. Today, our logistical network stretches from the factory to the foxhole, and the means of controlling that network exist almost exclusively in the cyber domain—from the operational commander initiating a supply action to the enterprise tracking that item from receipt of request through delivery.

This logistical thread ties the modern battlespace together, and an adversary's ability to untie these connections to counter American power significantly dampens our inherent advantages and limits our freedom of action. Military planners often falsely assume that we will not face a contested environment until we are attempting to enter a theater, encouraged by military language that speaks to anti-access and area denial, and not global counter-power projection. Planners routinely look for an adversary to affect us with an arsenal of advanced capability-denying weapons like integrated air defense systems, anti-ship missiles or mines, intermediate-range or inter-continental ballistic missiles, or other kinetic forces. However, this assumption fails to address the universal applicability of the cyber domain in transregional, multi-domain conflict, and the ways modern technologies could extend conflict to the homeland.

Gaining a better understanding of the impact that cyber could have on our operations requires these planners to imagine a 21st century, Russo–Japanese War, or comparable scenario, in which we struggle to project power beyond the homeland. In our case, it would be a scenario where ships never leave port and aircraft never leave the runway; one where the planned, overwhelming force simply never leaves our shores. To prevent what would most certainly result in strategic shock, USTRANSCOM defines the changing battlespace for counter-power projection as the "contested environment," where adversaries continuously dispute American power across all domains, linked by the cyber-enabled delivery chain. With that definition, we are able to imagine concepts previously unfathomable and remain at the cutting edge of strategic thought.

Often exclusively understood as a specific engagement area or warzone, the contested environment actually extends across the vast array of organizations that deliver a force, from the continental United States to the warfighter. Digital tools and technology inform every step in the deployment process, creating multiple levels of possible interference. Since services, agencies, and Combatant Commands all observe risk differently, DOD's challenge is to use this expanded definition of "contested environment" to inform assessments and prioritize resources. In USTRANSCOM, accomplishing national objectives means reevaluating assumptions and addressing the potential for a deteriorating asymmetric advantage in strategic mobility. Assessing strategic risk in contested environments enables governmental agencies to highlight each other's needs and vulnerabilities. This cooperation, in turn, enables the mitigation and coordination required to project power globally, particularly across the cyber domain. More importantly, strategic risk assessments highlight the operational planning considerations required to prioritize and defend global mobility assets, networks, and cyber infrastructure.

Leading the Way

Malicious cyber actors increasingly pose the greatest asymmetric threat to American military supremacy. Without superiority in the cyber domain, it will not matter how dominant the Joint Force is; if we cannot project power, then it does not matter how much of it we have. The USTRANSCOM team recognizes the need to seize the cyber initiative to safeguard transportation operations across all other domains, and to ensure operations through our strategic ports, rail corridors, road networks, and distribution nodes. Many of our Joint Force customers do not realize that the bulk of the force moves on commercial carriers whose information systems are even more vulnerable to cyber threats than hardened military networks. Therefore, we must change the way we view the character of war to preserve American dominance, assure the mission, and preserve military options and decision space for the U.S. President in the 21st century.

It is fair to say that only a short time ago, USTRANSCOM was admiring the cyber problem. Today, USTRANSCOM is on the leading edge of facing the challenge by developing the programs, processes, and personnel to address digital disruption threats. Russia's strategic mistake in 1904 was a failure to plan for rapid deployment, and today this means securing cyberspace. The inherent task for USTRANSCOM is to broaden the scope of its analysis into an assessment of hazards and responsibilities by actively evaluating the most vulnerable aspects of our command and control, systems, and infrastructure. In today's connected world, this assessment infuses digital awareness as a core principle of mission success and highlights the need for a resilient cyber network. Ultimately, our job is to assess these vulnerabilities and provide multiple options for the Joint Force while creating multiple dilemmas for the adversary.

With an area of responsibility that transcends geographic boundaries, USTRANSCOM began its cyber journey by realizing that the cyber domain forms the connective tissue of our entire distribution network. We reached this understanding by educating our leadership and key teammates. We invited experts from government, industry, and academia to participate in a series of cybersecurity roundtables. These experts included heads of cybersecurity firms, Chief Information Officers, scholars, and talented hackers. With their assistance, we began to shape a vision of mission assurance in cyber-threatened and cyber-degraded environments. These cybersecurity roundtables are now biannual events, designed to continuously expand the Command's perspective and establish a foundation for actionable progress.

USTRANSCOM also conducted its first "thin line" cyber assessment in 2016 and outlined how to employ fundamental security strategies and develop the means to deny or respond to cyber events. The thin line is the operating space that separates our key cyber terrain and infrastructure from an adversary's ability to affect our operations—a cradle-to-grave look at where our mission incurs risk from cyber. This first thin-line assessment also tackled hard challenges, such as the Command's reliance on commercial providers across disparate virtual infrastructures. Taking this broad view allowed us to expose numerous seams between military and commercial networks, quantify our limited authorities, and appreciate the implication of DOD cyber standards that do not necessarily extend to industry. As a result, we are institutionalizing and accelerating our ability to conduct similar assessments while moving forward to secure network data across applications, protecting our mission-critical information. While the task was initially daunting in scope, a holistic approach helped us capture both the breadth of effort required and the depth of organizational impact. It also reinforced the need to treat cyberspace operations as central to mission assurance. After mapping out our critical cyber infrastructure and corporate relationships, USTRANSCOM successfully partnered with organizations like Defense Digital Services (DDS), Stanford University's "Hacking for Defense," and DOD's Strategic Capabilities Office (SCO) to better inform our cybersecurity needs and help us develop innovative solutions to some of our most pressing challenges.

Today, USTRANSCOM is refining its Cyber Mission Assurance Strategy and actively pursuing initiatives to bolster mission critical capabilities. In conjunction with DOD, Combatant Commands, services, and interagency partners, we identified and analyzed key cyber terrain to assist with prioritizing support from our limited cyber forces. We enhanced security protocols and better defined relationships with our commercial providers and government partners. USTRANSCOM is also path-finding the next generation of cybersecurity, thinking through vital cyber considerations in war games and simulations. We are correcting outdated assumptions about permissive operations, and as a result, developing an all-inclusive enterprise view of critical cyber roles and tasks. Our goal is to position every mission partner across our organization to see themselves contributing in one or more cyber lines of effort, to deliver digital mission assurance and inform our situational awareness.

However, cybersecurity means more than addressing current network needs. We must also protect our data and continue to improve our capabilities as technology develops. With an eye to the future, USTRANSCOM is leading DOD by adopting a cloud-based infrastructure that enables better encryption, empowers trusted transactions, enhances data management, increases storage, and scales network demands to support our unique logistical requirements. We know we have to stay at the forefront of the Department's focus on multi-domain conflict, continuously infusing cyber resiliency into our distribution mindset. Working with our Joint and commercial partners, we are developing a more robust, decentralized, and agile cyber infrastructure that provides cyber security and preserves our ability to move and sustain superior forces.

What is Next

The future of cybersecurity has three strategic defensive focus areas, each meant to address and progress network survivability: resilience, deterrence, and technology. By focusing on these three survivability areas, USTRANSCOM can prevent the digital disruption of its distribution network and protect against a contemporary equivalent of the Russian failures deploying to Port Arthur. Resilience strategies are those that maximize our ability to detect hostile actions and control damage. This approach includes real-time network monitoring and response, either through a user-driven or automated function, allowing quicker recovery. In promoting a reactive role, we accept risk in unclassified data, but this is critical to our ability to remain interconnected with our commercial providers. Deterrence strategies limit access or minimize network exposure to deny an adversary access to our systems. Though deterrence strategies have the benefit of effectively closing opportunities to the adversary, they restrict our own organic operations because of restrictions on connectivity.

In blending resilience and deterrence strategies together, a more complete mission assurance cyber strategy understanding emerges—we can expect a certain level of interference from an adversary, but we still seek to limit that access. The path to accomplish this is through the third focus area, the advancement of our technological capabilities. The cyber domain is growing at an ever-increasing rate, shortening the time span from state-of-the-art to obsolete each day. To operate effectively within our distribution network, we must stay at the forefront of this dynamic cyber transformation, continuously seeking out new ways to secure our operations. This task starts by harnessing the power that resides within our own data. It is not sufficient to simply digitize our existing activities—we have to leverage the data.

That said, when discussing data, we have to make an important distinction. Data should not be treated as mere information. Rather, data is living material, shaped through critical insights and aligned with key parameters to inform tasks. In USTRANSCOM, our data revolve around connecting the user to the supplier and the distribution network. We recently began the first steps of mapping and pooling our data into a proverbial "lake" to initiate the creation of accessible, annotated, and useful knowledge. This business intelligence will work to improve and optimize the management of our enterprise, enabling and promoting computer-guided gains in efficiency, flexibility, and effectiveness. A robust neural net of algorithms will advance our data and create the potential for machine learning and artificial intelligence, to anticipate, predict, and proactively respond to our needs. As self-sustaining technology, our networks would detect deviations and intrusions while refining their own software and algorithms, improving performance in real-time while enabling immediate threat response.

The evolution of big data analytics is what makes it "smart." By compressing the time from analysis to action, we can eclipse the human advantage and an adversary's ability to disrupt operations in a contested environment. In the not-too-distant future, machine learning will allow us to process information, identify shortfalls, and enable corrective action before human ability can detect a threat. As USTRANSCOM builds its data lake, we are transforming our cyber vulnerabilities from limitations to knowledge. With this groundbreaking shift in how we process information, we are also expanding the potential for autonomous systems and vehicles. Autonomy provides an incredible capacity to leverage data-driven, global situational awareness to better disperse our network vulnerabilities and promote resilience. In this manner, autonomy is the action arm of smart data, and it represents the most significant present-day disruptor to commercial transportation capabilities and capacity. Autonomous vehicles have the power to streamline the number of pilots, sailors, and drivers we need, minimizing risk and cost while allowing us to capitalize on industry's technological gains.

> *Though deterrence strategies have the benefit of effectively closing opportunities to the adversary, they restrict our own organic operations because of restrictions on connectivity.*

A Call to Arms

If we ignore the cyber domain's role in our ability to project power and perform critical supply and sustainment missions, the adversary gains an easily exploitable advantage. As a result, we can no longer assume away delivery and transportation challenges. With a cybersecurity focus, USTRANSCOM will continue to perform its mission and enable the fulfillment of national objectives: delivering an immediate force expeditiously and a decisive force when needed—anywhere, anytime, all the time.

However, USTRANSCOM's efforts are not enough—we cannot address cybersecurity in isolation. Leaders across industry and government will ultimately decide how to address the cyber threat as it continues to evolve and affect operations in yet undetermined ways. Commanders need to advocate constantly for senior leader attention on contested environments and cyber mission assurance problemsets. If an organization is not engaged in addressing cyber domain challenges, it cannot expect to dominate its competition. Prioritization is just one way to bring cyber to the forefront of an organization's focus.

Senior executive leaders should also pursue comprehensive workforce development and training to enable our cyber operators to remain relevant. We cannot expect to maintain an advantage in multi-domain operations or move a force with digital tools if we do not have the right talent with the appropriate training. Workforce development and human capital management take on new meaning and value in an era where military success no longer exclusively relies on how much combat power one brings to the fight. Instead, success may hinge on how quickly one detects and resolves cyber intrusions. As an organization, we need the same skilled information technology workers as the successful start-ups of our day, with whom we compete for talent. The other part of our challenge is hiring the right number and the right mix of military and civilian personnel. By leveraging the skill of our workforce with emerging tools and collaborative technologies, we can better allocate duties and work, and give our people the necessary time to think—to anticipate, adapt, and guide the agile responses a distribution network requires in contested environments.

Commanders need to advocate constantly for senior leader attention on contested environments and cyber mission assurance problemsets. If an organization is not engaged in addressing cyber domain challenges, it cannot expect to dominate its competition.

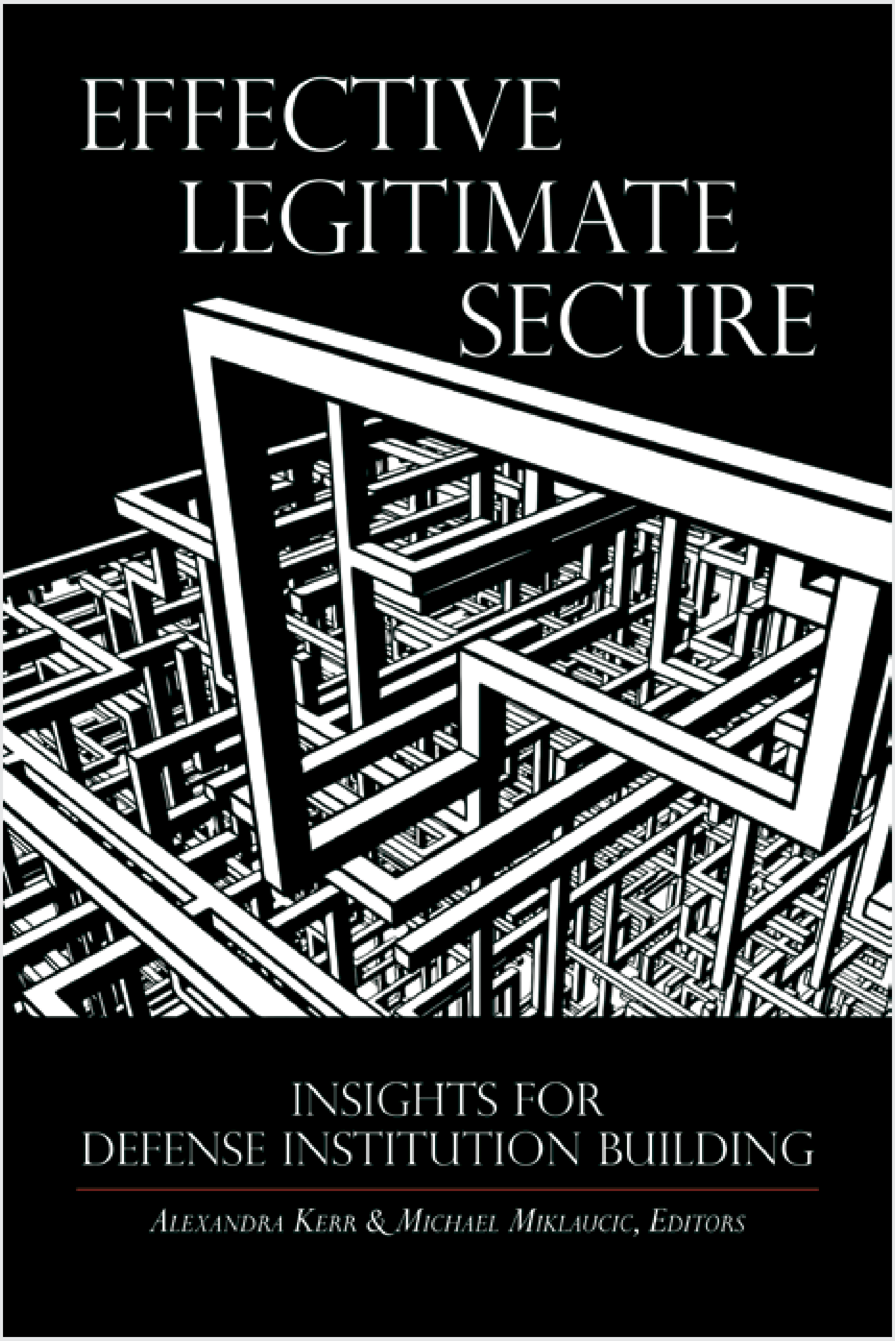
Buoyed by executive leadership advocacy and explicit workforce development, we advance the dialogue where cyber security is a pillar of mission assurance. In this vein, we should seek to collectively set and enforce digital standards for the hardware and software involved in our distribution network and those we do business with—how and where we design, manufacture, maintain, install, and connect systems. For USTRANSCOM, that means investing in the infrastructure that supports and delivers our warfighters while protecting its ability to provide options and solutions to complex delivery problems. We are in a battle to gather and process data at faster and faster rates, and to make informed decisions when confronted with these problems; this requires the intentional development of our cyber infrastructure. With a resilient and secure network, we will enable the Joint Force to develop and prepare for operations in contested environments, accept or mitigate strategic risk, synchronize operations, and deny an adversary from pursuing asymmetric advantages across all domains.

The Only Winning Move is to Play

Functional views of USTRANSCOM's Combatant Command role do not provide enough emphasis on the critical nature of our cyber networks and infrastructure, nor on the importance of the JDDE and Global Deployment Network within DOD. Our mission requirements transcend geographic Combatant Command areas of responsibility and necessitate the ability to project force wherever and whenever needed. By partnering with industry and innovative organizations to better understand our mobility requirements, USTRANSCOM can safeguard American power across contested domains. We need to imagine the art of the possible, exploring the latest capabilities to resolve our inefficiencies and educate our personnel. We need to continue to lead and foster relationships, to better understand the next tasks that will shape our digital future and raise the level of connection to our data. We need to promote a multi-domain endstate, not advocate for targeted advancements or stove-piped outcomes.

The more successful we are, the more our adversaries will attempt to contest our influence, having potentially catastrophic consequences. By pursuing cybersecurity as a means to ensure global power projection, the United States can preserve its superior advantage in conflict. These are not solely technical issues, nor are they owned by any single entity within the JDDE. These are strategic issues. Leaders at all levels must continue to address cyber-specific challenges and recognize the consequences of cybersecurity failures, both in our policy and in our operations. Together, we can create the unity of purpose and effort required to deliver solutions. As a result, our adversaries will have fewer opportunities to degrade our mission capability. Future attacks will be less likely to succeed, and if they do succeed in disrupting operations, we will effectively mitigate the impacts to our overall mission and to the Joint Force Commander's ability to execute.

To succeed in cyber, one must play the game. The ancient Chinese strategist and philosopher Sun Tzu famously noted, "To subdue the enemy without fighting is the acme of skill." The advent of advanced cyber capabilities and related gray zone activities make this concept appreciably more realistic and contemporary. Although the connectivity and transactional speed enabled by cyberspace have revolutionized the way we think about command and control, information sharing, and operations assessment, our growing dependence on digital tools creates tremendous vulnerability. Russia's defeat at Port Arthur more than century ago is a compelling example of the tyranny of distance and the consequences of allowing logistics to exist as an afterthought. The reality is that scores of similar examples permeate across history, highlighting the direct relationship between logistical shortcomings and strategic failure. Viewed through the lens of the changing digital battlespace, we depend on the cyber domain to project power. We simply cannot afford to ignore or downplay the threat. PRISM

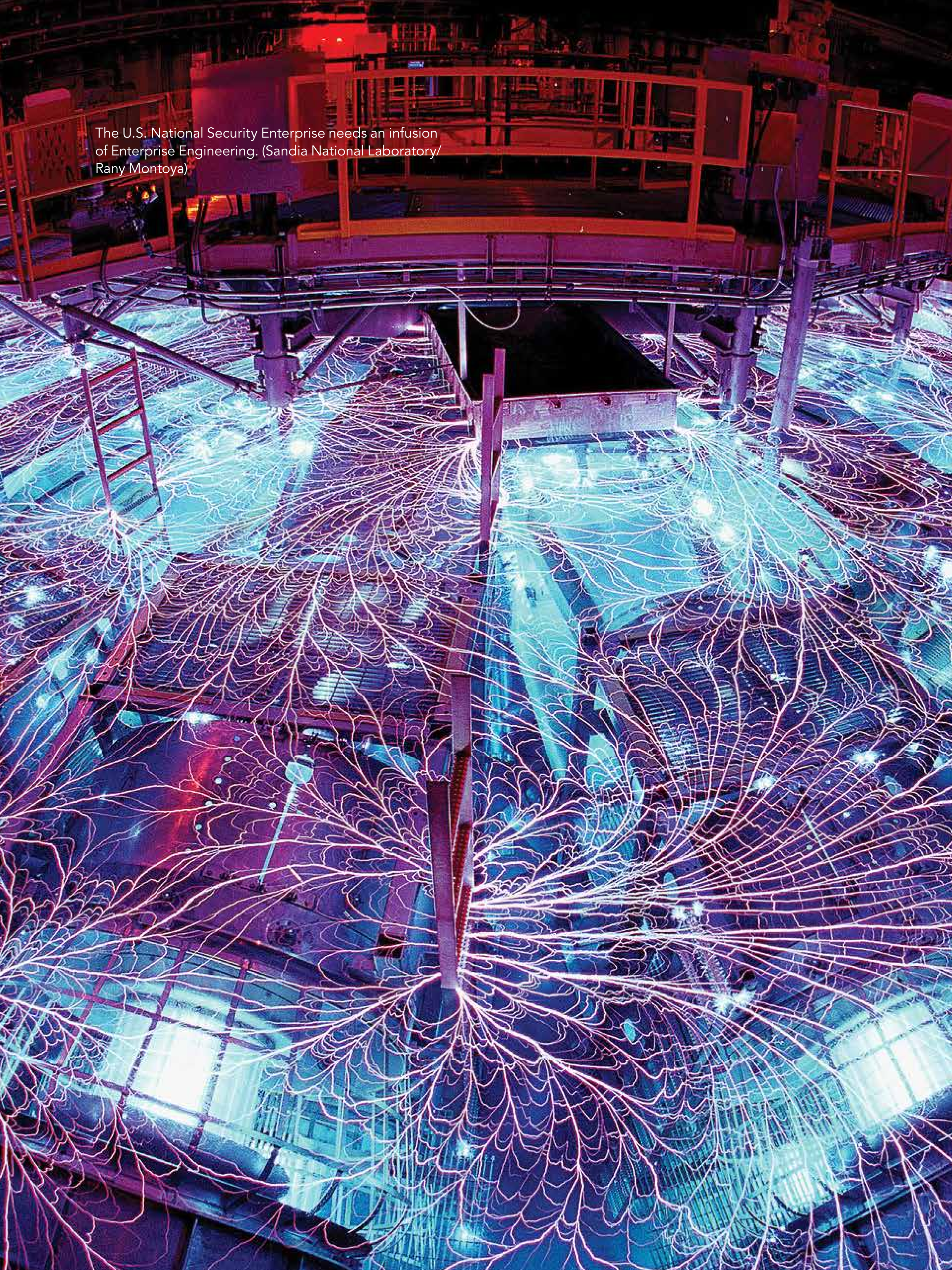


EFFECTIVE
LEGITIMATE
SECURE

INSIGHTS FOR
DEFENSE INSTITUTION BUILDING

Alexandra Kerr & Michael Miklaucic, Editors

Available online at <cco.ndu.edu>.



The U.S. National Security Enterprise needs an infusion of Enterprise Engineering. (Sandia National Laboratory/ Rany Montoya)

Digital Dimension Disruption

A National Security Enterprise Response

By Charles Rybeck, Lanny Cornwell, and Philip Sagan

The digital dimension is simultaneously enhancing and disrupting the fabric of life in every society where modern, *informatized* technology is present.[1] The slow-motion collapse of parts of the 20th century's legacy is now accelerating in ways that likely will usher in a monumental realignment of societal institutions, methods of business, and fundamental ideas about national security. This realignment will, of necessity, change the frameworks within which America provides for its security, including how it acquires the goods and services it uses in that effort.

The U.S. National Security Enterprise (NSE or Enterprise) has not yet grasped, as evidenced in budget priorities, what it means to live in a world where the threats reside at considerable distance, at scales beyond our imaginings, and at speeds that cannot be easily comprehended. Information technology has penetrated all aspects of our lives and the *informatized threat* is a clear and present danger. The People's Republic of China has penetrated our defense supply chain, North Korea has exposed our corporate vulnerabilities, and Russia has threatened our social cohesion. From a national security perspective informatized threats are by no means limited to the military or intelligence domains.

Yet the Enterprise thus far has followed predictable, requirements-driven, program-oriented constructs that attempt to "normalize" responses, which subdivides the problem too early and misjudges its scale.[2] What will it take to achieve enough common understanding to impel action? What will it take to align the NSE, its allies, and its partners to take effective, coordinated, and coherent countermeasures to maintain peace (when possible)?

The NSE needs an infusion of enterprise engineering originating within its most senior levels, to establish new rules of engagement that match the emerging threat. *Informatized conflict* redefines the battlespace and demands a comprehensive and coherent response. Success depends on the active engagement of the entire diplomatic, economic, and military arsenal. This article adopts the best current, unclassified, holistic view of an informatized era vision for the Enterprise.

Mr. Charles Rybeck, Mr. Lanny Cornwell, and Dr. Philip Sagan are senior advisors to the U.S. Intelligence Community and Department of Defense.

The Informatized Era

The word "computer" originally meant a person who did computation, like the clerks in 17th, 18th, and 19th century brokerages. Computing machines (what is now meant when anyone says "computers") emerged in the mid-20th century as a quantum leap forward in how humans did calculations and searched for information. In the past quarter century, human use of computers has changed fundamentally, but common terminology has not kept pace with reality.

Society has become almost wholly dependent on informatized systems. As part of the creative destruction/evolution that drives capitalism, the pre-informatized infrastructure has been destroyed, but societal processes—especially those of government, defense, and the law—are still those of the pre-informatized world, a world that is rapidly going out of existence. The world is using digitized, sharable information, transitioning from one-way, single-supplier siloed, one-function stovepipes to interactive ecosystems where software is orchestrating the movement of goods and services, the making of decisions, and impacting the way humans live. In just one generation, every industry has come to depend on interactive real-time decisionmaking.

A careful look at what has changed in the transition from the computer era to the informatized era reveals a qualitatively new infrastructure that matured during the past twenty years. Distance and time are compressed to the point where an adversary's geography is not decisive (or, in many cases, even discernable) and the pace of action can be so fast that it defies normal human cognition. Most U.S. citizens can identify aspects of this new infrastructure such as broadband connectivity, massive availability of compute power on a global basis via the cloud, and the advent of big data. However, the implications of the changes brought by informatization have not broken through to the thinking guiding the highest levels of the U.S. Government.

The informatized era's new infrastructure is distinguishing itself by freeing increasingly mercurial data to move around the world—from place to place, from purpose to purpose—to feed previously unimagined analytics. Indeed, the nature of data is, itself, undergoing a fundamental change. The terms "bespoke data" (from the British term for custom-tailored) and "by-product data" highlight the difference between data created in the old pre-computer and computer worlds and data created by or in the new informatized world.

Bespoke data are made by a human using measurement tools, like much of traditional intelligence, created to answer a known question. By-product data are incidentally created by machine operations, like the geolocation data dropped by smart phones, and are then available for other use. By-product data are growing exponentially as a primary feature of the informatized era, and are only in the infancy of exploitation by the NSE.

The Significance of Informatized Conflict

All informatized systems are essential to our national security irrespective of geography, or commercial or government origins. Informatized conflict includes all national security-relevant activity, both kinetic and non-kinetic, whether it is commonly understood by practitioners as being in that context or not.[3] For example, private commercial transactions are often conducted by their participants as if they had no national security implications. But all serious analysts recognize the indispensability of our critical infrastructure, including the electronic systems that facilitate commerce.

As anyone with a smart phone knows, the digital dimension is now integral to every aspect of business and societal interaction on a global scale. Viewed through the lens of informatized conflict, the "information technology" (IT) concept clearly fails to capture the full impact of the digital dimension on our world. The concept harkens back to the now-distant days when IT was a sequestered, relatively unimportant, compartment of our world. Chief Information Officers (CIOs) reported to Chief Financial Officers (CFOs) because Chief Executive Officers (CEOs) pigeonholed computers as simple aids to accounting.

While many summarize current threats under the term "cyber," a concept that points to everything digital, the terms "digital" and "cyber" are insufficient to capture the current threat dynamic. Cyber, for example, has usefully come to point specifically at computer network operations (CNO), but fails to capture the digital dimension as a whole. CNO's commonly described sub-divisions—computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA)—and encompass only a subset of the digital foundations on which modern life is being built.

Alignment—Develop Informatized Fusion

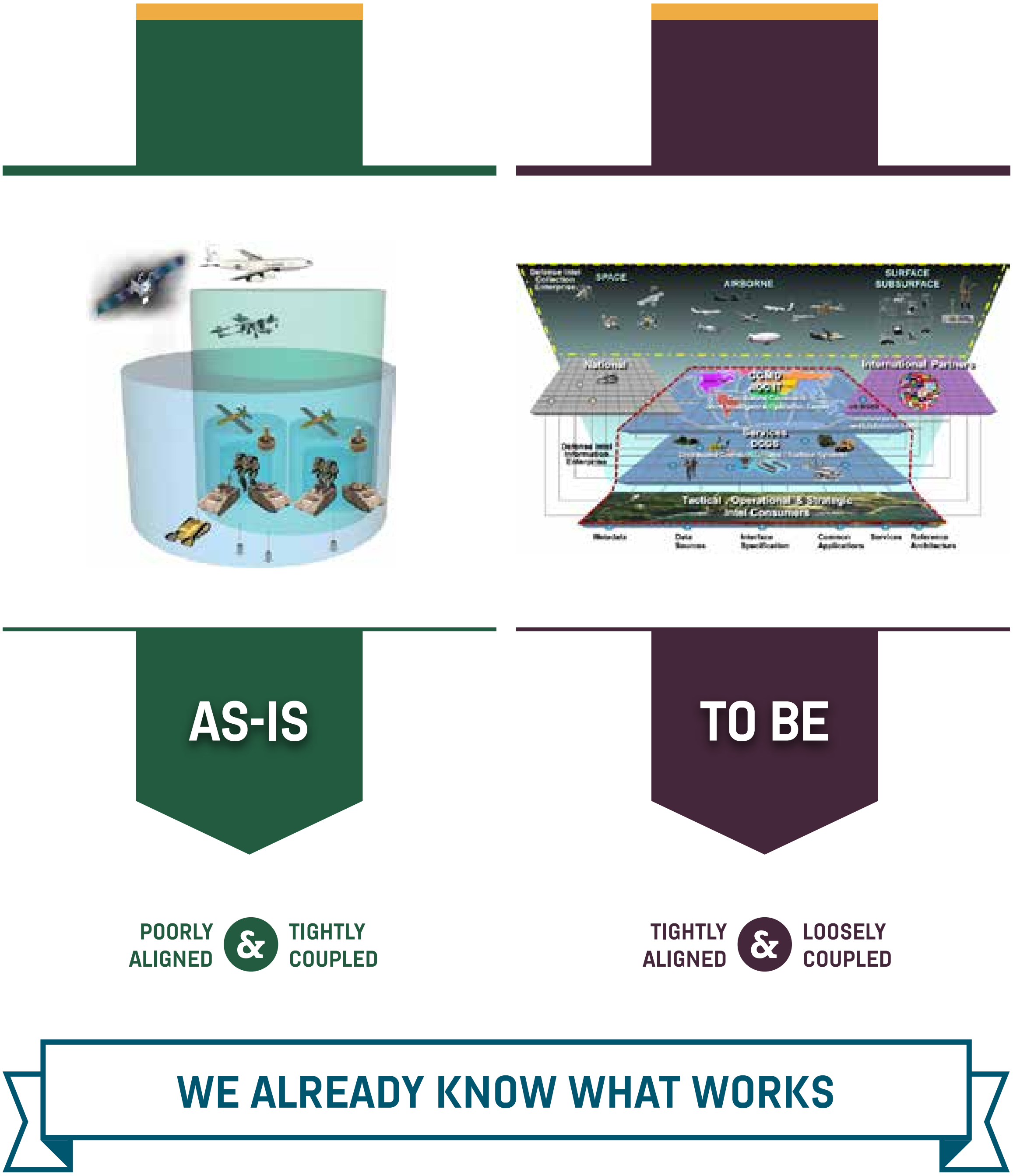
America entrusts its frontline national defense leadership to the Department of Defense (DOD) and the Intelligence Community (IC), two interconnected but separate chains of command. These entities are chartered to deliver kinetic and non-kinetic capabilities. Only the Commander-in-Chief (POTUS) controls both. As hard as it is for POTUS to exert Commander's intent, Congress faces even greater impediments when it attempts to prompt changes to how DOD prosecutes its mission. For example, Goldwater–Nichols (the U.S. Department of Defense Reorganization Act of 1986) demanded jointness in our military, and Clinger–Cohen (the Information Technology Management Reform Act of 1996) demanded IT rationalization.[4] Neither the White House nor the Congress have directed DOD or the IC with sufficient clarity to guide execution of these for the 21st century.

DOD and IC systems are compartmentalized and often impervious to improvement with industry best practices. The lefthand image on Figure 1 depicts how the NSE platforms, sensors, and weapon systems are siloed and disjointed. Every unit in the IC and DOD is sub-dividing the Enterprise problem and producing their own examples of this poorly aligned and tightly coupled approach. A massive array of programs and projects have been given carte blanche to operate using proprietary systems, creating processes that, while often narrowly effective, are impervious to improvement by informatized standards. In addition, the leaders of these programs are incentivized based on quick wins and continued resource growth, but these small pockets of capability do not add up to an Enterprise solution.

The righthand image in Figure 1 combines the vision of then Undersecretary of Defense for Intelligence James Clapper for intelligence, surveillance, and reconnaissance (ISR) with all projections of national power. This vision has not been translated into a full-blown strategy and does not yet represent the NSE reality. It does, however, provide a strong basis for the fusion of command, control, communications, computers, intelligence, surveillance, and reconnaissance.[5]

This vision of an informatized era "to be" depicts the alignment as it is required at the top and center of the Enterprise. Subsequent to that alignment, an unlimited number of loosely coupled implementations at the edge can then seamlessly connect and interoperate. This "tightly aligned/loosely coupled" engineering approach has been successfully applied at the Enterprise level in the private sector to guide foundational, internet-dependent initiatives. In less than three decades, for example, this approach has proven itself to be the most effective way for informatization to transform global enterprises, including Wal Mart, Netflix, and Google.[6] It explains not only how the internet works, but is

FIGURE 1: Tightly Aligned/Loosely Coupled as a Winning Joint Strategy.


Defense Intel Collection Enterprise
SPACE
AIRBORNE
SURFACE
SUBSURFACE
National
International Partners
Services
DCGS
Defense Intel Information Enterprise
Tactical, Operational & Strategic
Intel Consumers
Metadata
Data Sources
Interface Specification
Common Applications
Services
Reference Architecture
AS-IS
POORLY ALIGNED & TIGHTLY COUPLED
TO BE
TIGHTLY ALIGNED & LOOSELY COUPLED
WE ALREADY KNOW WHAT WORKS

ideally suited to support "innovation at the edge" for American warfighters.

Jointness in the informatized era needs to refer not only to the combined efforts of our armed services but also to the unified actions of DOD, the IC, and other stakeholders—and their ever-shifting alliances—whose efforts combine in pursuit of national security with all the instruments of national power. And fusion will need to combine data, data science, and data services to achieve the security objectives first outlined by the bipartisan 9/11 Commission.

Informatized fusion thus describes the new core competence that the NSE must develop to prevail in informatized conflict. The Chinese and the Russians have already adopted their variants of informatized fusion as guiding strategies.[7] As a democracy, however, the United States requires popular understanding and support to pursue this strategy. Fortunately, the United States variant can maintain its comparative advantage by drawing on inherent American strengths—namely constitutionally protected rights as well as checks and balances built into three branches of government, private sector competition, the rule of law, and multi-ethnic diversity.

In the words of former Director of the Central Intelligence Agency Michael Hayden, America needs to balance "unity of effort"—i.e. tight alignment—with "autonomy of action"—i.e. loose coupling. This new, agile, non-stovepiped approach to national security related actions would allow asynchronous, near real-time intervention outside today's cumbersome processes. This vision is often cited in non-authoritative documents, but it has not yet been translated into a clear Commander's Intent, Congressional Intent, or the guiding National Strategy, nor has it been realized. Unfortunately, if America stays on its present course, it is not likely to get there. Now is the time to exploit a "tightly aligned/ loosely coupled" strategy to fortify the NSE.

Mobilization—Champions Enable

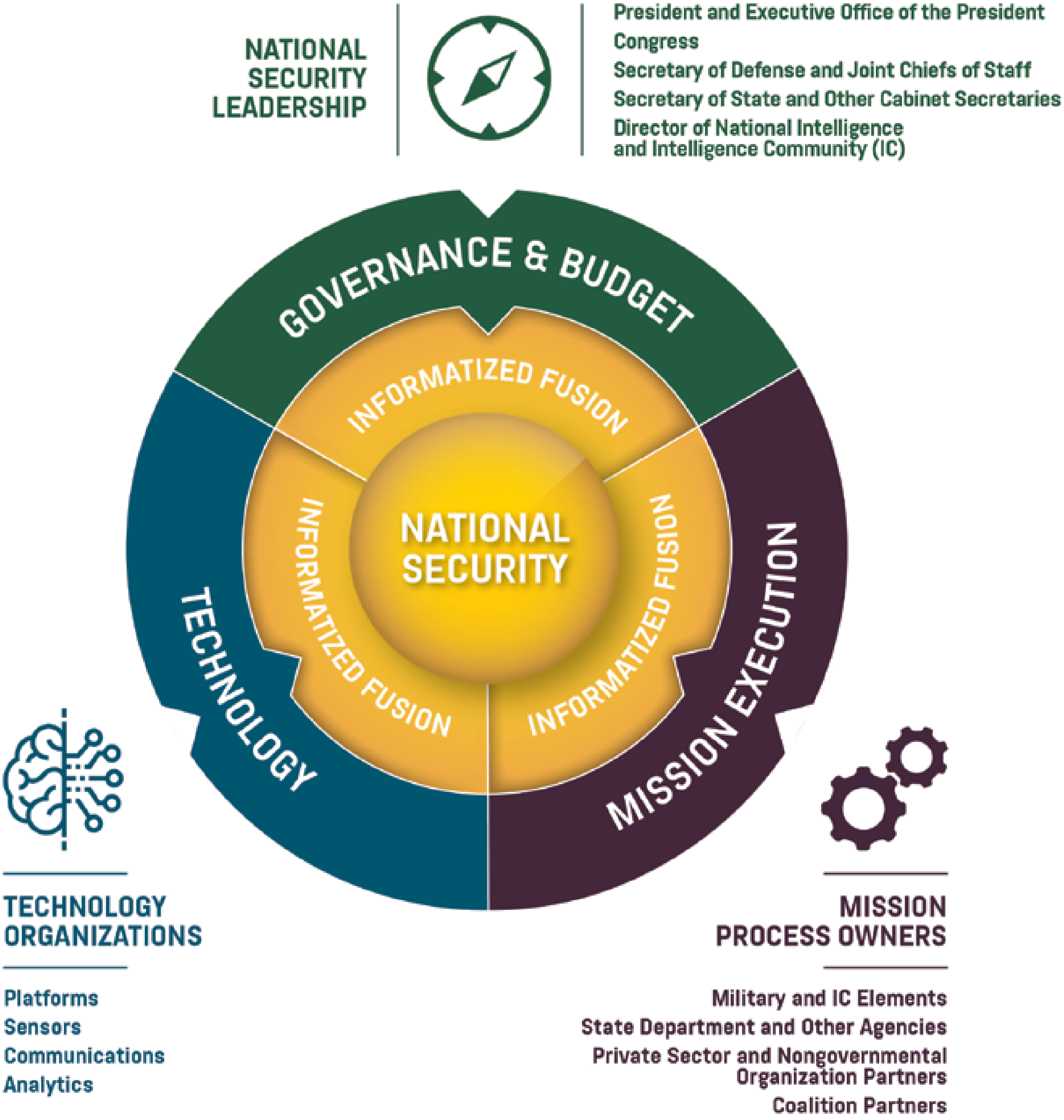
To be fair, this process has already begun at levels lower than the Enterprise as a whole, with sponsorship at lower levels and with charters, leadership, and budgets insufficient to the larger task.[9] Mission success is achieved only through authorizing initiatives at sufficient altitudes to match their charters and assigning responsibility to executives of sufficient gravitas. Informatization era challenges have their roots in the technology arena, but business-as-usual technological solutions alone will not address these challenges.

Decisionmakers and influencers from across the executive and legislative branches, with the support of the American public—will have to consider, adopt, and develop a joint 21st century vision to realize the benefits of this digital reorientation. Champions are the only ones eligible to align and mobilize in the service of jointness as redefined here to include the entire NSE.

Government governance and budget, mission execution, and technology elements perform functions analogous to their three familiar private sector equivalents—i.e. the CEO Team, the Chief Operating Officer (COO) Team, and the CIO Team. These three mission-critical teams shown in Figure 2 combine to form the NSE and fulfill its mission. Any mission-critical team can initiate Enterprise-level innovation, but it is the joint action of all three together that delivers the Enterprise-level benefits.

The differences between the government's organization and the private sector—e.g. the shared powers of Congress and POTUS—are useful in understanding why commonsense solutions and efficiencies adopted almost universally in the private sector cannot be easily adopted by the government. Informatized fusion as a joint strategy would implement mechanisms for aligning all three mission-critical areas, expedite Enterprise-level solutions, and incorporate appropriate checks and balances into the decisionmaking process.

FIGURE 2: The National Security Enterprise's Three Mission-Critical Teams.



NATIONAL SECURITY LEADERSHIP

President and Executive Office of the President
Congress
Secretary of Defense and Joint Chiefs of Staff
Secretary of State and Other Cabinet Secretaries
Director of National Intelligence and Intelligence Community (IC)

TECHNOLOGY ORGANIZATIONS

Platforms
Sensors
Communications
Analytics

MISSION PROCESS OWNERS

Military and IC Elements
State Department and Other Agencies
Private Sector and Nongovernmental Organization Partners
Coalition Partners

Ultimately, the Commander-in-Chief and Congress will need to mobilize the three mission-critical teams to meet the challenge of the digital dimension. To some observers this will look like reprogramming, to others it will present itself as major changes to mission processes, and for still others it will appear as technology transformation. To all those involved, however, it will reflect unprecedented alignment. This fusion demands cross-functional experience to fully accommodate their counterparts' frames of reference, demands, or "battle rhythms." Only a few, exceptional individuals in the government possess the required competencies—vision of the end game; cross-functional credibility; and maturity born of experience with sustained and disciplined innovation at the highest levels—to galvanize support and align stakeholders around the mission. The champions of this strategy will require a Senior Executive Technical Review and be empowered to act on its findings.[10] At the operational level, these champions will have to:

- Articulate a full-blown informatized fusion vision that matches the task and continually reminds everyone who will listen why the larger initiative is being undertaken.
- Align the vision's mission/business case (with quantitative and qualitative analysis of its risks and rewards) with its concept of operations and reference architecture.
- Arrange sufficient and sustained funding for all key elements of the initiative. Weak organizations use the mission/business case only to justify initial funding. Strong ones see a persistent, living mission/business case as a primary tool for guidance and for ensuring the delivery of promised benefits.
- Sequence activities based on announced priorities and predecessor/successor relationships to make sure benefits are delivered as promised. Only by delivering a no-kidding "without this…" list can a champion confront stakeholders with the stark reality of what it will take to achieve the benefits the champion presents in the corresponding and contingent "…you do not get that" list.
- Prioritize and communicate realistic expectations.
- Empower and incentivize executives at all levels when they enable shared, Enterprise-focused mission capabilities, and disincentivize silo-oriented approaches.

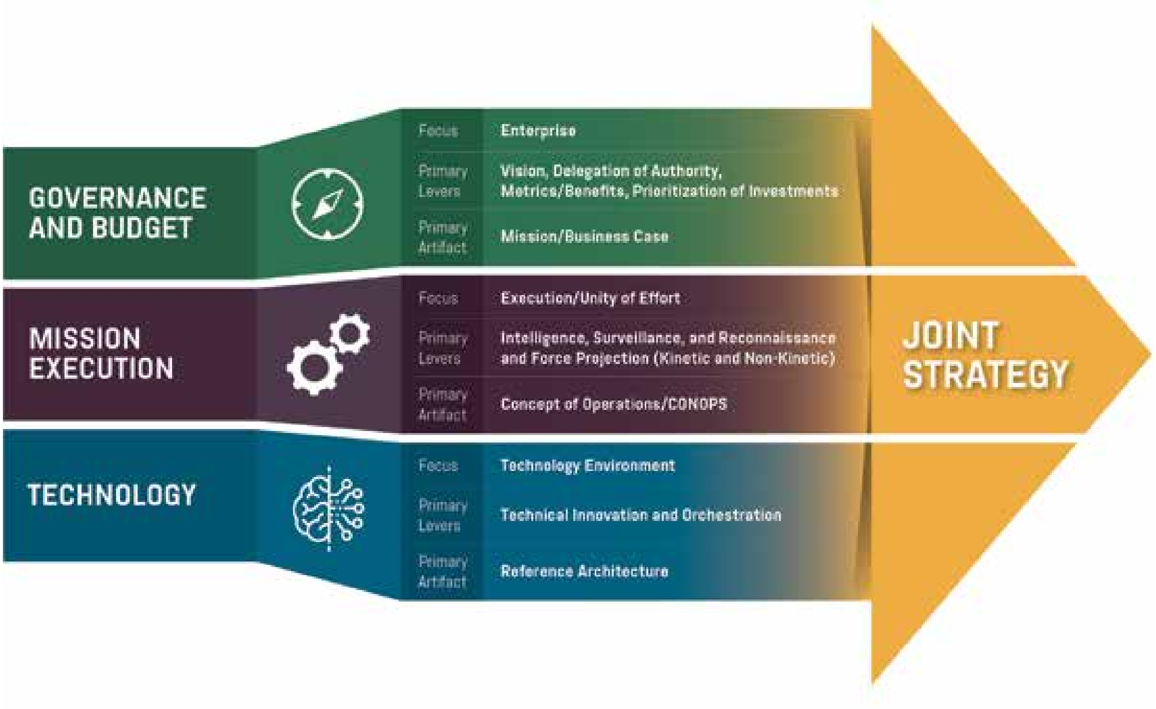
What are the Primary Levers for Informatized Fusion?

Figure 3 summarizes the NSE's response to informatization, making the "big rock" changes that the champions' levers will have to move to deliver mission benefits. The right champions will know how to use a rigorous "mission/business case" to sustain alignment among the three mission-critical teams and to sustain bipartisan support. They will need to alter the rules of engagement under which the entire NSE conducts its business.

Fortunately, the mission benefits are so powerful and the cost savings so dramatic that a coherent and well supported mission/business case at the informatized NSE level could overcome the entrenched interests who can be expected to fight it with all the tools at their disposal. Getting this right can unleash incredible growth and innovation. The potential may be compared with the 19th century commitment to build railway lines with a consistent gauge (the distance between the rails), which was an essential step in the growth to a unimodal, continental economic engine.

Many of the new rules of engagement require changes in processes where the NSE is employing 18th, 19th, and 20th century acquisition methodologies to solve contemporary, informatized problems that are mutating at an ever-increasing pace. Historic acquisition methodologies are not up to the current challenges, diminishing the NSE's

FIGURE 3: Aligning The Three Mission-Critical Teams.



GOVERNANCE AND BUDGET
Focus
Enterprise
Primary Levers
Vision, Delegation of Authority, Metrics/Benefits, Prioritization of Investments
Primary Artifact
Mission/Business Case
MISSION EXECUTION
Focus
Execution/Unity of Effort
Primary Levers
Intelligence, Surveillance, and Reconnaissance and Force Projection (Kinetic and Non-Kinetic)
Primary Artifact
Concept of Operations/CONOPS
TECHNOLOGY
Focus
Technology Environment
Primary Levers
Technical Innovation and Orchestration
Primary Artifact
Reference Architecture
JOINT STRATEGY

ability to keep up with, let alone get ahead of the rapidly rising, digitally-driven, innovation curve.

In the computer age, the NSE sought unique stand-alone things. While sometimes extraordinary, these solutions had pre-defined and relatively fixed capabilities, making them ill-suited to adapt with the changing needs of the stakeholders. In the informatized age, the focus has shifted toward integrated capabilities, solutions built on commodity technology. Even though these new informatization-aware systems are driven by specific missions, their capabilities are built to relentlessly adapt with the ever-changing needs of NSE-wide stakeholders.

Government champions as described in this article, alone, have the authority to prosecute informatized fusion and all it implies. Only they can move the biggest rocks, the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR), so that the NSE can coordinate—at the digital dimension level—procurement and deployment of virtually everything. With strong leadership, the NSE can rapidly transition from acquiring extraordinary things that confer relatively fixed capabilities to open-ended, increasingly extraordinary capabilities built using commodity things. U.S. Air Force Space Command has already begun to shift from buying rockets (things with capabilities) to buying launches (capabilities).

In the absence of fully engaged champions, the NSE routinely avoids discussion of the cross-cutting capabilities on which informatized fusion depends. Lower-level government employees are not empowered or incentivized to operate at the scale or scope required to make the needed changes in either process or procurement. They are left waiting until aligned senior executive champions intervene to exercise their extraordinary and non-routine authority, changing the rules of how business is conducted. Until then, lower-level employees are reduced to reporting classic quick wins and low-hanging fruit. Until their boss' bosses make the tough choices and substantial investments needed for informatized fusion, the oft-touted mission benefits will remain elusive.

Future Proofing the NSE

To ensure that the results of the champions' actions endure, this article looks to enterprise engineering—a discipline that makes practical application of systems engineering at the organization level, directing a venture in its entirety as a system-of-systems. It considers every aspect of the Enterprise, including business processes, information flows, material flows, organizational structure, and the human condition.

Our Constitution represents one of the most successful and earliest examples of enterprise engineering. To ensure that the NSE has the resiliency to informatized change that gives it a lifespan comparable to that of the Constitution, the NSE needs an infusion of enterprise engineering originating in the most senior levels, establishing new rules of engagement that recognize the world is now irreversibly informatized.

The history of successful reengineering of processes within the national security arena has almost invariably been associated with mission process owners who were empowered to make the necessary changes. A good—though all-too-rarely-remembered—example was provided by Admiral Hyman Rickover, the father of the Navy's nuclear propulsion program. Because Rickover was so widely respected and because his authority was so significant, he was able to serve the NSE as an invaluable counterweight to the contractors who were building the ships, ultimately forcing the adoption of the standardized solutions required to achieve Enterprise-level alignment.

Rare exceptions only prove the rule: wherever process ownership is unassigned—as it is throughout most of the NSE on most national security processes—process improvement is left homeless, without adequate guidance and context. ARPANET—the defense network that became the basis of the internet—demonstrated a means of exerting sufficient guidance and control to enhance the likelihood for success without stifiling innovation or slowing the pace of change. ARPANET offered unprecedented connectivity and revolutionized information architecture. Here the structure (packets in defined forms), flow (transmission), and management (orchestration) of information was transformed into what we all now recognize as the underlying foundation on which the modern internet is built.

Enterprise engineering has always required so much more than just managing the underlying technology. Whether dealing with the internet or the electrical grid, the private sector had to work with the public sector to set the standards. Subsequently, all enterprises (public and private) had to make major investments to adapt their business practices to take advantage of the new infrastructure.

History shows that establishing foundational alignment cannot be accomplished through business-as-usual channels. Extraordinary interventions by the most senior executives—who, under business-as-usual conditions, typically have little involvement with infrastructure—was what proved decisive. Only after alignment was achieved through regularizing the structure, flow, and management of information could the work of adapting systems for exploiting that infrastructure be delegated. In the case of informatized fusion (combining cloud, mass analytics, and the projection of national power), the NSE will need to align around changes in the structure, flow, and management of information to begin what will be an ongoing process.

The NSE's current unaligned objectives, budgets, programs, policies, and procedures limit successful examples of enterprise engineering to isolated islands. Only an "automagic fallacy" would suggest that such disparate efforts would produce informatized fusion. The NSE simply cannot afford to wait until adversaries inflict catastrophic damage before it strategically aligns and takes the steps that it already knows are needed. In advance of the unthinkable, can America do what it takes to provide for the common defense in this era of informatized conflict? PRISM

Notes

[1] Informatized is that quality—of any hardware, software, platform, sensor, process, organization, service, or device—of being digitally informed and digitally vulnerable, based on being interconnected, digitally interactive, and remotely controllable. Informatized systems are susceptible to digital input, output, influence, coordination, or orchestration, whether or not these characteristics are apparent. This article defines the term informatization and related constructs beyond their common usage by the Chinese (and beyond the original work by the Office of Net Assessment in the U.S. Department of Defense, from which the Chinese derived so much) and enhances these constructs to convey importance to our NSE. The article chose the shortened English form of the Chinese term xinxihua, "informationized" or "informatized" and combines it with "conflict." Limited and specialized terms such as "warfare," "combat," and "operations,"—the terms that the Chinese have paired with xinxihua—do not capture the ubiquity of what is being informatized. Here, "conflict" is a catchword to encompass everything involved in disputes with national security implications. For an extensive discussion of these issues: See Andrew F. Krepinevich, and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy*, (Basic Books, 2015).

[2] Will Roper, Ph.D., the head of the Strategic Capabilities Office in the Office of the Sectary of Defense communicated the relevant imperative succinctly as, "Don't [prematurely] subdivide the problem." Presentation at May 19, 2017 Joint Staff Industry Day held at the National Geospatial–Intelligence Agency.

[3] A 2014 paper "Military Competition and Conflict in the Information Age: Asymmetries between US and Chinese Conceptualizations of Information Operations" by Barry Watts of the Center for Strategic and Budgetary Assessment (CSBA) explores the Chinese strategic and practical insight in detail.

…The Chinese ideographs such as 信息化作战 have produced a variety of English translations, 'informationized operations' and 'informatized operations' being the most common. A more literal translation is 'information technology-based combat.'

…the US military does not have terms or overarching concepts as comprehensive, coherent and well thought through as Chinese notions of 'informationized operations' and 'informationized war' (xinxihua zhanzheng) in local, high-technology (high-tech) wars under 'informationized' conditions.

Revolution in Military Affairs (RMA) breakthroughs by the Soviet Union were studied and converted for use by the United States by Andy Marshall at the Pentagon and others in the 1970s, 80s, and 90s. These insights served as a basis for many of the US advanced technology achievements of those years. Paradoxically, the Chinese drew on and are currently drawing on the work of Andy Marshall and other Americans to develop their informatized warfare construct and strategy (what this article calls informatized fusion), while America is lagging behind.

[4] The Goldwater–Nichols Department of Defense Reorganization Act of 1986, Pub.L. No. 99–433; the Clinger–Cohen Act or the Information Technology Management Reform Act of 1996, was part of the National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104–106.

[5] Fusion is the seamless aggregation, merging, or combination of multiple, disparate inputs into a single process for a coordinated mission purpose.

[6] Major retailers and service delivery firms (for example, WalMart in the 1990s and Netflix in the 2000s) rebuilt their supply chains using this approach. Google acquired Android in 2005. Its software, used on smartphones, tablets, and other devices, is the operating system (OS) with the world's largest installed base. Each of these businesses created a "platform" that today serves as the basis of unique business model success.

[7] For more information on China's efforts see: Fravel, M. Taylor. "China's New Military Strategy: 'Winning Informationized Local Wars'." *Browser Download This Paper* (2015).

[8] Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, (Penguin, 2016), 177.

[9] The CIA's establishment in 2015 of its Directorate of Digital Innovation (DDI), which brought the CIO and

multiple operational units together under Mission leadership) and the DNI's Intelligence Community Information Technology Enterprise initiative (which is orchestrating new infrastructure) were both examples of necessary but insufficient efforts.

[10] This "Senior Executive Technical Review" notion jars many Government leaders. There are few precedents for bringing together programmatic leads with the technical and execution leads. But without convening such expertise, the USG is left spending massively without successfully meeting the informatized conflict threat. But, acting together, the President and Congress can create this new, informatized era precedent.

Past examples are not comparable to the challenges today, but these examples are instructive. For example, Philip Zelikow brought together luminaries at the level we are proposing for the work of the Markle Foundation and the 9/11 Commission. These groups addressed complex technology and interagency challenges, translating classified and technical understandings into unclassified policy prescriptions in laymen's terms. Additionally, during World War II the U.S. President asked James F. Byrnes to leave the Supreme Court and lead what became the Office of War Mobilization in 1943.

Photos

Page 40. Image of an X-Ray Machine by Rany Montoya at the Sandia National Laboratory, available at <https://www.flickr.com/photos/departmentofenergy/8056998596/in/album-72157630137563548/>. Photo unaltered.

Cybersecurity experts at the Lawrence Livermore and Berkley National Laboratories are leading a program to develop new data analysis methods to distinguish between power grid failures caused by cyberattacks and failures caused by other means. (Lawrence Livermore National Laboratory)

A Cyber Federal Deposit Insurance Corporation?

Achieving Enhanced National Security

By Dante Disparte

Of the emerging man-made risks affecting U.S. national security, cyber threats have enjoyed the most attention and resources from national security leaders and policymakers. And yet, cyber threats remain one of the most complex risks to address given their amorphous, highly fluid, and extra-territorial nature. This makes it difficult if not impossible to quantify the national state of readiness and, in these fiscally constrained times, the return on investment from the billions spent each year on cybersecurity. Five gaps conspire to make achieving a state of enhanced cyber resilience complex if not impossible. These include a yawning talent gap to the tune of millions of people; a technological gap predicated on managing a risk that evolves according to Moore's law; a financial and economic gap leaving trillions in value at risk with no generally accepted way to measure this value; an alignment gap in terms of policy harmonization and cooperation inside the United States and around the world; and, finally, a gap in patience and the speed of markets. This article delves into the evolving cyber threat landscape and outlines ways of understanding and bridging these critical gaps.

Shared Risk, Shared Defense

The United States enjoys an undeniable economic and national security advantage from being the birthplace of the internet and, with it, the midwife of the digital age. These advantages have been reaped since the early 1990s, where the road to building a 21st century economy began—connected at every turn, person, node, and device to a worldwide web of risk and reward. The United States has since remained the world's economic supremo and, for a period after the global financial crisis, the only functioning cylinder in the global economy. But will this *pax digitalis* hold or is U.S. national security and economic prevalence waning because of the blowback from our marvelous creation?

Today, it is hard to imagine a world without the internet and without the hyper connectivity it has enabled. Indeed, technology titans such as Facebook's Mark Zuckerberg and Amazon's Jeff Bezos look every bit the part of 21st century business statesmen.[1] Speculation of presidential runs from Silicon Valley's independently wealthy and decidedly pro-digital elite suggests that the line between public policy, the

Mr. Dante A. Disparte is founder and Chief Executive Officer of Risk Cooperative and serves on the board of the American Security Project.

digital commons, privacy, and security may be forever blurred—especially in the eyes of millions of millennials whose newly minted political engagement treats the internet as a utility, and privacy as a tradable right. This is troubling because the world is beset by a growing number of challenges pitting privacy and security advocates against one another, much as we saw with the now infamous case of "Apple vs. the Federal Bureau of Investigation" or in the Snowden leaks, which revealed wide-scale digital eavesdropping on the U.S. public—albeit at the metadata level, as security proponents argue.[2]

Just as privacy and security represent key policy, security, and business tradeoffs, connectivity and national cybersecurity are similarly dialectical choices. On the one hand, the tide of connectivity cannot be reversed. Indeed, with the explosion of connected devices, the so-called Internet of Things (IoT), people seem almost reflexive in their acceptance of a technological front door (and back door) to every tangible item in their life.[3] The annual Consumer Electronics Show (CES), is at once the digital sycophant's dream and the cybersecurity hermit's nightmare, as each connected gewgaw and curio is revealed to a fawning public and a salivating shareholder. According to Gartner, there are 8.4 billion connected devices in 2017, a 31 percent increase over last year. This exponential growth of connectivity, much as we saw with the Dyn exploit that shutdown the websites of major firms such as, Netflix and CNN, IoT will expand both the attack surface area and vectors that can not only take down much of the internet, but exfiltrate sensitive information, cripple critical systems and sow misinformation.[4] Indeed, concerted efforts to exploit our connectivity and obsessive news media cycle still cast a long shadow over the 2016 presidential election and the current administration.[5]

And yet, rolling back the tide of digital connectivity would represent the loss of trillions in economic value in the global economy, accepting that much of what financial markets trade in is notional. Firms like Amazon, which has recently acquired Whole Foods in a $13.7 billion transaction that was quickly netted out by Amazon's share price gains, will command 50 percent of all U.S. e-commerce by 2021.[6] Firms like Facebook have quickly transformed into a service that is fast becoming tantamount to a digital census of more than 2 billion people—growing monthly active users at a rapid rate, many of whom enjoy their solitude in the company of others.[7] Firms like Google are not only synonymous with the web, they have quickly morphed into a modern *keiretsu* under its new *nom de guerre* Alphabet, to deploy their considerable human, technological, and financial capital toward redefining the future. Firms like Apple and Tesla are similarly poised to not only command the present, but very much shape the future—one where the digital divide between man and machine is being bridged by wearables, augmented reality (AR), and artificial intelligence (AI). In this near-future the *uncanny valley* no longer scares us and the very morality, proximity, and humanity of warfare is being lost to drones and digital threats.[8]

Modern commerce is very much a tale of creators and accelerators. Where iconic firms like Ford took more than century to reach $45 billion market capitalization, Tesla—a comparatively young upstart of a mere 14 years of age—has overtaken Ford in valuation despite Ford's 100 year-long head start.[9] With this shift in what can be described as digital industrial production comes a raft of unforeseen exposures, such as those posed by mechanical and process autonomy. Driverless cars and self-driven features are already present in thousands of vehicles on U.S. roads and around the world. Indeed, the concept of self-driven road convoys of large tractor trailers is well beyond the conceptual and piloting stage and now entering commercial viability.[10] With the advent of industrial autonomy comes a profoundly vexing era of redefining individual responsibility, third party liability and product safety standards—one which many a trial attorney and jurist are preparing to litigate. In the highest order, this new normal should also herald the emergence of digital democrats, citizens and politicians who are not only conversant in technology, but possess the technical virtuosity to steer the world with their vote and vision while navigating the potential disruption of hundreds of millions of jobs, thousands of industries, all asset classes, and national security.

The robber barons of the Industrial Age unwittingly triggered man-made climate change through their ravenous pursuit of a carbon-based economy. Likewise, the early adopters of the internet have gained incalculable wealth while unwittingly opening a Pandora's Box of cyber threats. The proponents of IoT, industrial automation, and AI are exposing the world to an increasingly complex and interconnected new normal that even has many of its greatest beneficiaries, such as Elon Musk, Tesla's CEO, and Eric Schmidt, Google's former CEO and Chairman of its parent company Alphabet, sounding the alarm.[11] While Musk is worried for humanity's very survival, which is why he is so feverishly attacking the internal combustion engine, AI, and commercial space flight, Schmidt has a decidedly more sobering—if somewhat convenient—assessment that data is the new oil, for which countries will likely go to war.[12] The opening salvo of this grim new normal was very much the Sony Entertainment cyberattack in 2014, which experts suggest was perpetrated by North Korea's cyber warfare arm under the banner "Guardians of the Peace."[13]

Sony Entertainment drew the ire of a nation-state by the none too flattering film *The Interview*, which, among other transgressions, depicted North Korea's dictator, Kim Jong-Un as an imbecilic character who was eventually assassinated. Allegedly in response, a full-scale cyber onslaught was launched against Sony Entertainment and, in many respects, its entire value chain in an effort to thwart the film's release. As the release date neared, a very sophisticated business model ransom attack was carried out with the threatened release of sensitive material, crippling systems and, ultimately, threatening movie theaters and movie goers, among others. This attack not only pitted Sony Entertainment against a nation-backed actor, the equivalent of having financial services firm Cantor Fitzgerald go after al-Qaeda after 9/11, it pitted President Obama against Sony's executives, in his public exhortation that they not give in to pressure.[14] In the end, this may have been a Pyrrhic victory for North Korea, as a film that would have been forgotten, is now documented in history books, and millions more viewed it as a result.

While the case was eventually resolved, it augured a new era of cyber risk and the increased likelihood of cyber warfare and terrorism. Our Achilles' heel was laid bare around five critical gaps in our national cybersecurity posture. The first, which was revealed in Sony's case, was the lack of a competent—literate and numerate—cybersecurity talent pool. The second was a clear technological gap not only in the defenses applied in this case, but in the clear double standard in who was to be covered by cybersecurity rules inside Sony and elsewhere. The third was the economic gap that emerged as the financial losses from this event were a mere rounding error in Sony's global earnings, but a material threat downstream in movie theaters and among actors, who not only feared for their privacy, they feared being caught up in the dragnet. The final two gaps are perhaps the most important, especially as the purview of response was in the hands of the U.S. Government and not a private enterprise. That is the lack of alignment on national security policies and how they interplay with the private sector. Finally, as with all man-made risk, of which cyber threats are one, the attacker has the benefit of patience and agency, while our economy blindingly moves forward at the speed of markets.

Talent Gap

Beyond Binary Code

For a risk that often emanates between the keyboard and a chair or through the greedy or nefarious motives of insiders, talented people are a critical link in the chain of cyber resilience. Underscoring how vital a "neural safety network" can be, the exploit of the SWIFT banking system, in which cyber criminals absconded with more than $80 million from Bangladesh's central bank accounts, was halted by an alert clerk at a corresponding bank in Germany. In this case, a heist that was nearing $850 million in attempted withdrawals was stopped because the clerk noticed the word "foundation" was misspelled and promptly alerted authorities.[15] It is difficult to "machine-learn" this level of pattern recognition and intuition, as most machines are learning that humans are error prone and might have forgiven the misspelling allowing the cyber capers to carry on. More than pattern recognition, risk management relies on culture and value systems, which are uniquely human traits.

> *Globally there is a cybersecurity talent shortfall of 1.5 million people. The United States is not spared from a yawning talent gap of more than 200,000 professionals who are not only needed to fill existing vacancies in one of the fastest growing fields, but are needed to define the standards of the future.*

Globally there is a cybersecurity talent shortfall of 1.5 million people.[16] The United States is not spared from a yawning talent gap of more than 200,000 professionals who are not only needed to fill existing vacancies in one of the fastest growing fields, but are needed to define the standards of the future.[17] This gap is not aided by an inwardly looking immigration and visa policy, which has diminished the U.S. beacon to the world's most promising professionals. Confronting cyber risk head-on is not merely about binary code, although so few have achieved the level of technical virtuosity needed to fully understand cyber threats and how to manage them. Cyber resilience also requires retooling even the most senior business leaders (from the board room on down) and policymakers on how to set up response, governance, and decisionmaking parameters around a threat that does not respect quorum, is infinitely connected, and can spread like a digital wild fire. The emergence of cyber risk governance executive education is a cornerstone of a safer future.

From Hundreds to Millions

Fighting a digital wild fire requires a digital fire brigade. As the WannaCry ransomware demonstrated during a weekend in 2017, cyber threats can spread across borders and across enterprises with blinding speed. Indeed, three days after news broke of this new ransomware payload that was being delivered using the Eternal Blue tool that was exfiltrated from the National Security Agency (NSA), it had affected systems in more than 150 countries.[18] While the attack and its meager ransom gains, payable in digital currencies like Bitcoin, proved to be a dud, it was nevertheless a major wakeup call that cyber risk was again metastasizing. The other gap revealed by the WannaCry attack was that everyone was in effect calling on the same scarce resource for comfort and resolution—namely, skilled cybersecurity professionals or those masquerading as experts due to paycheck persuasion or hubris.

If WannaCry were a rapidly spreading urban fire, there are simply not enough firefighters to keep properties safe. In addition to the lack of talented individuals, those who are out there are often hamstrung by financial constraints and the lack of leadership comprehension of how vital their roles really are. The cyber literate are often not numerate when it comes to defending the business cases that not only justify their existence, but their desired (or, better yet, required) investment levels. This is compounded by the growing "cyber arms race" taking place among nation-states, the public sector, and private enterprise, which is increasingly viewing cyber resilience as a source of competitive advantage. Imagine if volunteer fire brigades that protect all the "commons" of a city, were corralled by the highest bidders to only respond to their localized emergencies? Undoubtedly, this would make for a truly unsafe city and eventually the embers of the least secure would catch fire in the "safer" parts of town. Indeed, it was a heating and cooling vendor that left Target's technological back door open enabling the exfiltration of 110 million personally identifiable records and customer data points.[19] For this, Target's CEO paid the price of a slow descent with a golden parachute, while the firm continues to grapple with earning back customer trust. The same holds true with cybersecurity standards and the war for talent, which negates the reality that cyber threats are a shared risk for which a shared defense is needed. Simply put, cybersecurity, like urban fire safety requires a collective approach.

Bridging the Gap

As with bridging any span between two points, the first step is to understand the distance between them and the depths below. The cybersecurity talent gap is a critical national security priority. Evidence of this is the fact that most agencies of the U.S. Government, including the ones that are supposed to be the most secure, like NSA, which seems to be in a constant maelstrom of breaches and bad news, are in effect outsourcing much of their work to the private sector.[20] It is important to remember that Edward Snowden—a modern Benedict Arnold to some and a Paul Revere yelling "the big state is coming" to others—was a private contractor with top secret clearance. This personnel outsourcing effort is most vigorous in the cybersecurity and national security domains.

> *All too often we are learning, with calamitous effects, that cyber risk is as much a people-centric threat, as it is a technological one.*

The first pillar in bridging this gap must be the emergence of sober leaders in the public and private sectors who treat cyber risk as a systemic threat.[21] These leaders must break down the organizational silos that relegate cyber risk to their often underfunded and unprepared information technology (IT) departments as a purely technological dilemma. These IT leaders in turn labor under the powerful inducements of hubris and paycheck persuasion. All too often we are learning, with calamitous effects, that cyber risk is as much a people-centric threat, as it is a technological one. For this, well-trained people must become a critical link in the common chain of cyber resilience.[22] Attracting this workforce in the United States and from around the world requires confronting the algorithmic hiring patterns that dominate talent development today. All too often recruiters or machine-learning algorithms are weeding out viable candidates for the lack of undergraduate or graduate education, in the search for "safe bets."

Similarly, the credentialing and skills development options available to the workforce are often too costly, unwieldy, or they labor under impractical, dated curricula that fail to keep pace with a risk that evolves according to Moore's law. Standing up an adequate cybersecurity fire brigade and its rank and file leadership will require tradeoffs and an uncomfortable degree of fluidity of talent and information sharing between the military, government, private sector, and academia. Vitally, a common lexicon around cyber risk governance is beginning to emerge, wherein senior leaders are beginning to realize that they are all too often the only ones left in the smoking crater of these intangible threats. Hitting third rails, like the Sony Entertainment breach or the 2016 electoral malfeasance will enable U.S. national security, public policy, and private sector leaders to begin to course correct and address our cybersecurity talent shortfall.

Technology Gap

Unicorns and Other Mythical Creatures

When it comes to cybersecurity the concept of a perfect technological cure-all is a near impossibility. This calls into question the investment thesis and inflated market valuations of many technology solutions purporting to offer a digital approach to cyber hygiene. This thesis and many aspects of the flood of capital and balance sheets that are on-risk in the cybersecurity market may very well produce a range of correlated losses or a complete crash.

Both the adversaries they face and the technologies that are used to deliver cyberattack payloads have the advantage of patience and Moore's law on their side. Similarly, the Achilles' heel of all technological tripwires is human behavior, which not only drives value-creation in the private sector, it drives decisionmaking and service provision in the public domain. In short, as experts assert, even the best cybersecurity solutions may fall to the four horsemen of human cybersecurity behavior, namely: curiosity, nescience, apathy, and hubris. The counterbalance then is a blended approach to cyber risk management that incorporates a continuum of security, beginning at the values and governance layers and ending with a fortified virtual wall and exit alarms guarding against the exfiltration of sensitive information.

Not Zero-Sum

Just as humans and human behavior can be the weakest link in the cybersecurity chain, over-reliance on technology can be as dangerous by creating a placebo for safety. For many firms, such as JP Morgan Chase, which spends more than $600 million a year on cybersecurity, the amount spent on cyber hygiene has become a proxy for safety.[23] The danger with this approach, however, is that there is a veritable cyber arms and defense race taking place among companies and countries. Rather than viewing cybersecurity as a shared service matching a shared risk, technology solutions have become hyper competitive, hindering interoperability, creating excessive firewalls (real and virtual), and attracting billions in capital from investors and customers chasing yield or reasonable assurances. Notwithstanding this flood of capital in the cybersecurity market, it is safe to assume most organizations in the world are already exposed to latent cyber threats.[24]

The reality with cyber risk and, therefore, cybersecurity technologies, is that it does not have to be a zero-sum proposition. Indeed, as we are seeing all too often with global cyberattacks and patient dark supply chain exploits, the lack of a common defense leaves many systems vulnerable.[25] Supply chains, critical infrastructure, and the other "commons" the global economy relies on to trade are in the cross-hairs of an insidious, water-like, and incredibly patient menace. Against this threat, technology plays a vital role; however, technology developers and investors must stop chasing unicorns to make handsome short-term returns. Instead, they must emphasize the development and roll out of solutions that are as ubiquitous as the threat. The key attributes of this enduring class of technology solutions is that they fade to the background of human and organizational activity. The more real or perceived interference with the way people work, the higher the likelihood people will find "cheats" around the friction. Like capital, human apathy together with our uncanny ability to not follow rules flows through the path of least resistance.

Supply chains, critical infrastructure, and the other "commons" the global economy relies on to trade are in the cross-hairs of an insidious, water-like, and incredibly patient menace. Against this threat, technology plays a vital role; however, technology developers and investors must stop chasing unicorns to make handsome short-term returns. Instead, they must emphasize the development and roll out of solutions that are as ubiquitous as the threat.

Bridging the Gap

So how do we bridge the multi-billion-dollar technology gap? The first step is to temper the marketing and development standards war raging in the cybersecurity marketplace. The failure of one industry peer, such as a bank with lower security standards, will erode confidence in all banking institutions. Herein lies a major challenge. How many credit unions or community banks can afford stratospheric spending patterns or adhere to onerous regulatory requirements, which are now incorporating steep punitive measures? One solution would be to develop the technological equivalent of a cyber Federal Deposit Insurance Corporation (FDIC).[26] While there are several bodies, such as the National Institute of Standards and Technology (NIST) trying to codify best demonstrated practices for cybersecurity, the challenge is that small-to-medium sized enterprises struggle to overcome a financial and human capital gap to keep pace with these requirements. Furthermore, the changes and best demonstrated practices continue to evolve. The best many business leaders can hope for—subject to IT hubris and paycheck persuasion—is the assurance of a "clean bill of health" from weary IT leaders, who themselves are struggling to keep pace.

A cyber FDIC, like the real FDIC, would be much more than a clearing house for assurance, it would be an entity where risk can be shifted in the aggregate, particularly for smaller and more vulnerable sectors of the economy or for critical infrastructure. Just as identity theft was largely defanged when banks coalesced around a zero-liability proposition for consumers, the threat of online fraud quickly gave way and the multi-trillion dollar online marketplace was born. As with all risks, we must constantly weigh the costs and benefits of proposed rules and technological solutions and remain especially cautious of so-called technological unicorns promising to be a perfect cyber risk cure-all.

Most of the best practices around cybersecurity are entirely free and based more on education and behavioral hygiene than on technological spending. Keeping technology teams accountable for updating software patches, or teaching employees how to identify a phishing scam or Trojan Horse, for example, are first low-cost lines of defense. The other key is to quickly destigmatize breach reporting through the adoption of an "if you sense or see something, do something" philosophy. Threat intelligence and information sharing are the best ways for people to stay abreast of the rapidly evolving threat landscape, including law enforcement and intelligence officials. Best practices for disaster recovery and business continuity are similarly low-cost and easy to implement, especially given the advent of cloud-based solutions.

At a time when the world and its institutions—from business to government—face a precipitous erosion of trust combined with a constant onslaught of public misinformation, transparency is the greatest cure. For this, emerging technologies like blockchain, which underpin the boom of digital currencies of which Bitcoin is the preeminent digital mint, not only offer a secure alternative to traditional ways of organizing information; they create an unalterable public ledger using a distributed database across thousands of nodes. Another added benefit of this distributed approach is that blockchain can serve as a veritable disaster recovery and business continuity engine, being the equivalent of an informational "seed vault" for what cybersecurity professionals term as the "crown jewels;" or those data points or virtual assets (such as intellectual property) that are

CORE ELEMENTS OF A CYBER FDIC

- Governed by a code of conduct and clear value system
- Destigmatizes threat information sharing
- Aims to cap legal liability—particularly for vulnerable market sectors, such as middle-market companies
- Establishes a public-private structure that serves as a center of excellence
- Establishes proportional risk sharing and premium allocation, as well as the pooling and collecting of risk premia
- Reinsures catastrophic stop-loss coverage in the private market
- Serves as a technology clearinghouse vetting and disseminating emerging risk mitigation tools
- Conducts and benchmarks cyber stress tests
- Identifies and manages cyber threats to systemically important institutions (e.g. critical infrastructure, internet choke points, banking and financial markets among others)
- Trains, develops, and certifies providing reasonable assurance that standards of cyber hygiene are implemented

essential to an organization. While the adoption of this level of e-governance will be uncomfortable for most countries around the world, whose leaders have often profited handsomely in money or longevity from the opacity and byzantine nature of government, the demands of public accountability are growing increasingly restive. Political leaders have a choice then; proactively embrace transparency and accountability and the technologies that can make it so, or have it imposed upon them on the streets and in ballot boxes.

Economic Gap

The Weakest Link

Any discussion of resilience that does not include an economic component cannot be taken seriously. Resilience to complex risk requires a funding strategy should the threats rear their ugly heads. Failure to create a financial backstop often produces adverse long-range impacts hampering economic recovery. The Gulf region of the United States is still struggling to recover from hurricane Katrina and the BP oil spill more than 12 years later. More recently, the damage wrought by hurricane Harvey on Houston, may very well be the costliest natural disaster in U.S. history.[27] The economic consequences of cyber risk are no less complex to address. One of the chief issues in financially quantifying the true costs of cyber threats is that the world's understanding of valuing data and other intangible informational assets is nascent; so much so that only a small handful of thought leaders are building the approach to data valuation. Using a somewhat linear approach, Lloyd's, the world's specialty insurance market, estimates the upper end of the costs of cyberattacks at around $120 billion in a new report.[28] Taking in the second- and third-order costs however, the true figure may be into the trillions, as so much of the world's economic value is not only notional, it is locked in highly fluid electronically tradable instruments.[29]

A (Worthless) Priceless Asset

If Eric Schmidt's prognostications are correct that the world will go to war over data, how will we value the spoils of war? Oil wars by contrast are fought over a natural resource whose economic value is not only universally understood (in part because of scarcity), with common unitary valuation methods and third-party validation, its geostrategic terrain can be readily demarcated. Data enjoys no such parallels, which is where the war comparison ends. Data is undeniably valuable, but not all data is created equal, which is why it has thus far evaded economic or enterprise valuation approaches. Data is neither geographically bound nor is it scarce. Indeed, after the oceans and the sun, it may be the world's most abundant resource given our propensity to share and gather every single tidbit of information on the planet—from the absurd, like Instagram photos of our last meal, to the essential, like nuclear reactor safety readings.

The closest proxy for economic data valuation is to borrow a page from the types of financial stress tests regulators use on systemically important financial institutions (SIFIs). The largest banks in the world are the repository of most of the world's capital, which is why they are constantly in the crosshairs of cybercrime, insider threats, and evolving capital adequacy standards. Following the financial crisis of 2008, regulators adopted more stringent stress tests to see how large banks would respond to shocks. Similar shocks can be employed on organizations to gauge how they would respond if their data assets were rendered unusable and which other assets would be adversely affected. Through this method, we can begin to approximate the enterprise value of data (EvD) for the organization in question. While somewhat crude, this methodology can help organizations, policymakers, and national security leaders begin to modernize and layer their financial hedging strategies.

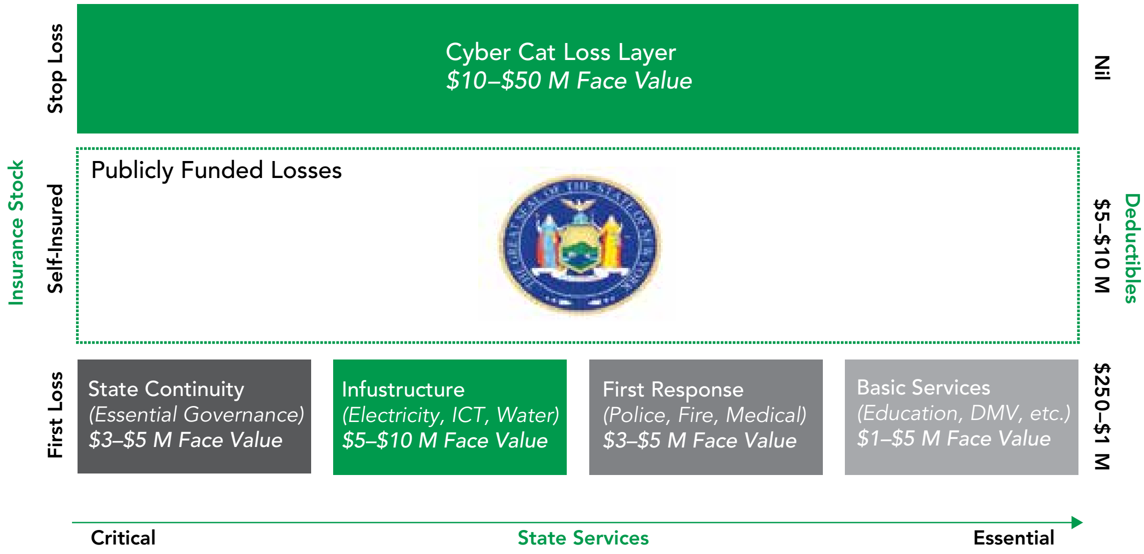
Modern Hedging

Cyber insurance is the fastest growing segment of the insurance market. While the first true cyber policies were placed at Lloyd's nearly two decades ago, insurers have experienced rapid market growth in the past five years. Today, more than 80 insurers are throwing their balance sheets at the cyber insurance segment. Despite this broad market participation on the supply side, the majority of cyber policies sold can be termed "Frankenstein" policies, or, rather, hybrid products where cyber is bundled with some underlying traditional class of insurance. One of the main challenges in guiding insureds through the appropriate risk hedging strategy is that most of the market views cyber risk and its attendant costs in a linear fashion. There is as much a gap on the supply as on the demand sides of the cyber insurance segment.

All too often customers seeking this coverage grapple with the question of "how much insurance to buy?" In most cases the math is troublingly linear. Firms will attempt to tally up the amount of personally identifiable information (PII) in their databases and then estimate a response and breach notification costs per record. On average, this produces a policy face value of $12 million across the U.S. market leaving most customers woefully under-hedged, especially when it relates to business continuity exposures, first party risks (or those events carried out by their staff—e.g. insider threats), and the growing incidence of cyber threats leaping through their virtual barriers causing physical damage losses.[30] All of these unfunded losses conspire to create a raft of litigation on denied cyber insurance claims, which in turn raises premium rates and increases the share of unfunded losses passed on to taxpayers or other parties.

To create a modern hedging strategy, the line between public and private losses must be drawn. After all, the public sector (often treated as a zero-liability entity) is increasingly behind some of the largest breaches recorded. The Office of Personnel Management (OPM), the U.S. Government's veritable human resources department was subject to the exfiltration of more than 21 million Federal employee records.[31] More recently, 200 million voting records for

FIGURE 1: Cyber Cat Loss Layer.



nearly all the U.S. voting public were exposed.[32] Additionally, the cyber exposure to critical infrastructure is fast becoming a real and present danger, from which the United States is not spared.[33] Hedging these costs calls for public–private risk sharing, wherein the concept of a catastrophic stop-loss solution can begin to adequately spread economic risks among willing insurers, making the government the insurer of last resort rather than the first line of defense. Figure 1 illustrates how this structure would be applied across agencies of a U.S. state.

Bridging the Gap

Bridging the economic gap posed by cyber threats is a clear national security priority. Unfunded losses in the private and public markets insidiously make their way to public funds, either in the form of failed firms and their attendant job loss and costs, or in the form of direct (unfunded) costs to local, state and federal agencies. Eventually the economic costs of cyber risk will have to be defrayed—or mutualized—across multiple stakeholders and market segments. A cyber FDIC that incorporates some share of losses, especially among the most vulnerable firms, cannot only offset costs, it can help spur better threat information sharing. Until then, recalibrating the adoption of standalone cyber insurance with clear terms and conditions can help reduce the share of these risks passed on to the public.

Eventually the economic costs of cyber risk will have to be defrayed—or mutualized—across multiple stakeholders and market segments. A cyber FDIC that incorporates some share of losses, especially among the most vulnerable firms, cannot only offset costs, it can help spur better threat information sharing.

Zen and the Art of Cybersecurity

If the gaps identified in this report are to be bridged, two vital support beams must be laid. The first is to align policy not only inside the U.S. and across all market sectors, but around the world. The transatlantic disconnect between the United States and Europe did not suffer its greatest blow with Brexit and the attendant EU schism, but rather with the upcoming implementation of the General Data Protection Regulation (GDPR) in Europe in May of 2018. These overarching cybersecurity and privacy rules, while far reaching and laudable for the centrality of individual privacy, adopt a carrot and stick approach to enforcement that may augur the equivalent of cybersecurity trade wars and privacy havens.[34] GDPR empowers EU regulators with a big stick, enabling them to levy fines of up to four percent of a firms' global revenues should they make any transgressions. Cybersecurity norms must be harmonized globally and threat information and the provenance of this stateless menace must be shared among authorities around the world and in near-real-time. The United States should lead this effort having woven the very fabric from which this scourge spreads.

However public policy and military doctrine evolve to respond to cyber threats, the path to enhanced national cybersecurity must be patiently charted. While our markets and personal demands call for immediate gratification, it is important to remember that cyber threats and the criminals, terrorists, and nations that collude with them have the benefit of patience and often lie dormant inside computer systems for years before they are discovered. To fight a patient, amorphous, and stateless menace will be one of the toughest challenges for public, private, and national security leaders. Just as the digital age has empowered ne'er-do-wells, it can also empower a new age of transparency, accountability and, above all, global cooperation to ensure the world's digital commons remain a force for good. Until then, our patience and mettle will be tested. PRISM

Notes

[1] Kate Vinton, "Jeff Bezos Overtakes Bill Gates To Become World's Richest Man," *Forbes*, July 27, 2017.

[2] Dante Disparte, "Apple vs. FBI: Much Ado About Nothing or a Temporary Truce?," *Huffington Post*, March, 31, 2016.

[3] Dante Disparte, "The I of very big T: (IoT Risks)," *Huffington Post*, August 19, 2017.

[4] Nicky Woolfe, "DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say," *The Guardian*, October, 26, 2016.

[5] Dante Disparte, "Free, Fair and (Mostly) Unfettered," *International Policy Digest*, November 16, 2016.

[6] Phil Wahba, "Amazon Will Make Up 50% of All U.S. E-Commerce by 2021," *Fortune*, April 10, 2017.

[7] Josh Constine, "Facebook now has 2 Billion Monthly Users and Responsibility," *TechCrunch*, June 27, 2017.

[8] In 1970 Tokyo Institute of Technology roboticist Masahiro Mori hypothesized that the more human a robot acted or looked, the more endearing it would be to a human being. See: Mashi Mori, "The Uncanny Valley," K.F. *IEEE Robotics and Automation Magazine*, 19 no.2. (2012).

[9] Patti Waldmeir and Richard Waters, "Tesla Overtakes Ford as Investors Bet on Electric Dream," *Financial Times*, April 3, 2017.

[10] James Vincent, "Self-driving Truck Convoy Completes its First Major Journey Across Europe," *The Verge*, April 7, 2016.

[11] Maureen Dowd, "Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse," *Vanity Fair*, April 2017.

[12] Tess Townsend and Eric Schmidt, "Big Data is so Powerful, Nation States Will Fight' Over It," *Recode*, March 8, 2017.

[13] Dante Disparte, "Welcome to 21st Century Warfare," *The Hill*, January 5, 2015.

[14] Greg Jaffey and Steven Mufson, "Obama Criticizes Sony's Decision to Pull 'The Interview'," *The Washington Post*, December 19, 2014.

[15] Kim Zetter, "That Insane, $81m Bangladesh Bank Heist? Here's What We Know, Wired," May 17, 2016.

[16] Van Zadelhoff, Marc, "Cybersecurity Has a Serious Talent Shortfall, Here's How to Fix It," *Harvard Business Review*, May 4, 2017.

[17] Steven Morgan, "One Million Cybersecurity Job Openings in 2016," *Forbes*, January 2, 2016.

[18] Dante Disparte, "WannaCry on Cyber Monday," *The Huffington Post*, May 14, 2017.

[19] Gregory Wallace, "HVAC Vendor Eyed as Entry Point for Target Breach," CNN, February 7, 2014.

[20] Les Williams, "Solving Government Outsourcing Risk with Private Sector Thinking," *International Policy Digest*, September 23, 2016.

[21] Dante Disparte and Les Williams, "Cybersecurity: The Next Sytemic Threat," *International Policy Digest*, April 12, 2017.

[22] Dante Disparte and Chris Furlow, "The Best Cybersecurity Training you can Make is Better Training," *Harvard Business Review*, May 16, 2017.

[23] Justine Brown, "8 Major Banks Join Forces on Cybersecurity," CIO Dive, August 11, 2016.

[24] Dante Disparte and Franzetti, Andres, "Learning Cyber Insurance Lessons from Life Insurance Underwriting," *Risk Management*, February 13, 2017.

[25] Dante Disparte, "Dark Supply Chains," *Huffington Post*, August 2, 2016.

[26] Dante Disparte, "It is Time for a Cyber FDIC," *Huffington Post*, June 16, 2015.

[27] Dante Disparte, "Hurricane Harvey: When Rain Bombs Go Nuclear," *Huffington Post*, August 29, 2017.

[28] Tim Worstall, "Lloyd's - Extreme Cyberattack Could Cost $120 Billion, as Much as 0.2% of Global GDP," *Forbes*, July 17, 2017.

[29] Dante Disparte and Daniel Wagner, "Do you Know What your Company's Data is Worth?" *Harvard Business Review*, September 16, 2016.

[30] Dante Disparte, "Virtual Threats, Real Consequences," *Huffington Post*, August 26, 2016.

[31] Kim Zetter, "The Massive OPM Hack Actually Hit 21 Million People," *Wired*, July 9, 2015.

[32] Aria Bendix, "GOP Firm Exposed U.S. Voters' Personal Data," *The Atlantic*, June 20, 2017.

[33] Caroline McDonald, "Cyber Blackout Could Cost Insurers $71 Billion, Lloyd's Reports," *Risk Management*, July 22, 2015.

[34] Dante Disparte and Chris Furlow, "GDPR and Information Security Arbitrage," *International Policy Digest*, August 24, 2017.

Photos

Page 52: Lawrence Livermore National Laboratory. Available at < https://www.llnl.gov/news/livermore-berkeley-labs-lead-project-increase-power-grid-cybersecurity>.

Cyber agent investigating a cyber intrusion. (FBI)

Bridging the Cyberspace Gap

Washington and Silicon Valley

By Adam Segal

One of the defining characteristics of the cyber domain is the dominance of the private sector. The majority of critical networks are privately owned and operated; more than 90 percent of American military and intelligence communications travel over privately owned backbone telecommunications networks. Many of the most talented hackers are in the private sector, and private security firms such as CrowdStrike, FireEye, and Cylance have taken an increasingly large public role in tracing cyberattacks to nation-states and other perpetrators. In addition, Alphabet, Amazon, Apple, Cisco, Facebook, IBM, Intel, and other companies drive innovation and the deployment of new technologies, especially in cutting-edge areas like artificial intelligence. For these reasons, strong ties to the technology sector are central to the U.S. Government's (USG) pursuit of its economic, diplomatic, and military strategic interests in cyberspace.

Until June 2013, there was an overlap of interests between Washington and Silicon Valley. There were, of course, political differences. The first generation of information and communication technology entrepreneurs had a strong libertarian bent, and saw policy as a distant concern, if not an outright impediment. Still, the two sides worked together to advocate for free speech and open access online, reduce international trade barriers, and promote the promises of the information technology revolution globally. They also had a strong interest in sharing threat intelligence and technical indicators from cyberattacks.

In June 2013, however, former National Security Agency (NSA) contractor Edward Snowden revealed U.S. intelligence gathering and cyber practices and operations, many of them targeted at U.S. internet platforms and software and hardware providers. During the Cold War, the United States targeted specialized networks and devices on a relatively limited set of targets used by the Soviet Union, China, and other adversaries. Today, military, government, commercial, and individual users all use the same commercially-sourced networks, computers, and devices. The data of terrorists, generals, foreign policymakers, or arms dealers are likely to travel along and be stored in commercial products, and as a result, Silicon Valley platforms are always going to be targets.

Motivated by a sense of betrayal, a commitment to an open internet, and economic interest, the technology companies have responded to the revelations by increasingly portraying themselves as global actors. Many

Mr. Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security and Director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

tech officials have argued for a more expansive definition of cybersecurity that focuses on the needs of all users and companies, rather than a more narrow definition centered on U.S. national security. In 2017, technology companies generated an estimated 60 percent of their revenues overseas. With their revenue increasingly dependent on foreign markets, especially China, there is also a strong motivation for the tech firms to demonstrate their independence from the USG.

The gap between Washington and Silicon Valley has only increased since 2013 after a number of public disputes.[1] In December 2015, a terrorist killed 14 people in San Bernardino, California. The Federal Bureau of Investigation (FBI) sought a court order to unlock one of the terrorist's iPhones. Apple protested, and public opinion was sharply divided over the balance between privacy and security. In January 2017, more than 125 technology companies joined an *amicus curiae* brief opposing President Trump's first executive order, which temporarily blocked all refugees and denied entry to citizens of seven predominantly Muslim countries. Tech company executives also expressed disappointment with President Trump's decision to withdraw from the Paris climate agreement; Elon Musk, the founder of SpaceX and Tesla, withdrew from two business councils providing advice to the administration on economic issues. Further driving the wedge between Washington and Silicon Valley, in June and July of the year, exploits developed from vulnerabilities discovered by the NSA were used in two large scale cyberattacks—WannaCry and NotPetya—that victimized the commercial sector and private users around the world, with losses totaling close to $8 billion by July 2017.[2]

The challenge of closing the divide is made even more pressing by the combination of a more assertive Chinese cyber diplomacy, the globalization of Chinese technology giants, and China's position as a leading hub for artificial intelligence research and development. After many years of reacting to Washington's efforts to shape cyberspace, Beijing has promoted a vision of governance centered on cyber sovereignty. As described by President Xi at the 2015 World Internet Conference in Wuzhen, China, cyber sovereignty means "respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet."[3] This position contrasts sharply with the vision held by the United States and its partners of cyberspace as an open, global platform, and has been furthered by commercial diplomacy and participation in forging international technical standards.

The Souring Relationship

Numerous countries have reacted to the Snowden disclosures by promoting industrial policies that avoid U.S. infrastructure, pressing for concessions from American technology companies, forcing companies to store data locally, or supporting domestic competitors. The Brazilian Government, for example, pushed forward plans for a new, high-capacity, fiber-optic cable connecting the Brazilian city of Fortaleza to Lisbon, Portugal, so as to prevent routing internet traffic through Miami. Moscow blocked access to LinkedIn after it failed to store Russian users' data locally. India pressed Microsoft for discounts of an estimated $50 million so users could upgrade to Windows 10 after the WannaCry and Petya cyberattacks.[4] In particular, Beijing has introduced several industrial policies as well as a national cybersecurity law designed to reduce dependence on foreign technology companies and promote local firms.

The technology companies responded to the disclosures with public outrage and efforts to hold the USG at arm's length through technology, legal challenges, and norms entrepreneurship. During the past three years, Apple, Microsoft, WhatsApp, and other companies have rolled out end-to-end encryption on smartphone operating systems, messaging services, and other online communications products. Data is scrambled in these products through mathematical formulas that the device manufacturer or service provider cannot reverse and recover data even when presented with a lawful warrant.

The move to encryption means that law enforcement and, to a lesser extent, intelligence agencies are unable to access data, even with a court order. In a March 2017 speech, for example, former FBI Director James Comey noted that in the last quarter of 2016, the FBI received 2,000 devices, and it was unable to access the data on 1,200 of them.[5] FBI and Department of Justice (DOJ) officials began warning about "going dark"—being unable to access data even with a warrant due to technological constraints—and to question the motivations of the technology companies.

In the face of this challenge, some federal agencies have called on U.S. technology companies to provide the technological means to bypass encryption, known as exceptional access or creating backdoors. These demands are not limited to the United States. After a Briton drove his car into pedestrians and attacked a police officer in March 2017, Home Secretary Amber Rudd said that intelligence agencies should have access to encrypted messages sent on WhatsApp. "We do want them to recognize that they have a responsibility to engage with government, to engage with law enforcement agencies when there is a terrorist situation," Rudd told the *BBC*. A few months later, German Interior Minister Thomas de Maizière announced that the German Government was preparing a new law that would give the authorities the right to decipher and read encrypted messages.

Tech companies have consistently argued that it is not possible to create backdoors without compromising the security of all users. Hackers and states will soon find ways of exploiting back doors. Or as Apple Chief Executive Officer Tim Cook put it, "You can't have a back door in the software because you can't have a back door that's only for the good guys."[7] Supporters of strong encryption also argue that neither the USG nor the private sector have a monopoly on encryption tools and methods. According to a Harvard University study, two-thirds of the nearly nine hundred hardware and software products that incorporate encryption have been built outside the United States.[8] Even if U.S. companies built in back doors, criminals and terrorists could easily use products developed elsewhere.

The technology companies have also mounted legal challenges to the USG's ability to collect data. Soon after the Snowden disclosures, Google and Microsoft filed motions with DOJ to be allowed to disclose how many times they had been ordered to share data with FISA. Microsoft also refused to comply with a Department of Justice demand for data from an Irish Outlook email account belonging to a suspect in a narcotics case. Microsoft argued that the data, stored in Ireland, was outside of U.S. jurisdiction and that requests for the information should go to the Government of Ireland.

On the legislative front, AOL, Apple, Facebook, Google, Microsoft, and Yahoo supported the *USA Freedom Act* and other legislative efforts to end bulk metadata collection of U.S. phone and data records. The Act, which was passed in June 2015, shifted bulk telephony metadata from the government to telecoms or private third parties. The same companies started a public campaign demanding "sensible limitations" on the ability of government agencies to compel tech companies to disclose user data. The companies argued, "Governments should limit surveillance to specific known users for lawful purposes, and should not undertake bulk data collection of internet communications."[9]

Technology companies have also taken a lead in defining and developing new norms of state behavior in cyberspace. In February 2017, Brad Smith, chief legal officer of Microsoft, gave a speech at the RSA cybersecurity conference calling for a Digital Geneva Convention "that will commit governments to protecting civilians from nation-state attacks in times of peace." Smith noted that one of the defining characteristics of the digital age is that cyberspace is produced, owned, secured, and operated by the private sector, and so the targets in cyberwar are private property owned by civilians. As a result, the tech companies act as "first responders" to nation-state attacks. In addition to deploying technical solutions such as encryption to fight state hacking, Smith called for the companies to "commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust."[10]

In the wake of the WannaCry ransomware attack, Microsoft also criticized the vulnerabilities equities process (VEP), the method through which the government decides whether to reveal vulnerabilities to the private sector or to hold on to them for intelligence gathering or offensive cyber operations. WannaCry, which encrypted data and held it captive until a ransom was paid, exploited a vulnerability that was allegedly developed by NSA and was offered online by a group known as Shadow Brokers. How this vulnerability and other tools made their way to Shadow Brokers, which is assumed to be a cover for Russian intelligence, is unknown.

Obama officials claimed that the default of the VEP, which involves representatives from the NSA, FBI, and Department of Homeland Security, is toward defense and disclosure. In a blog post in April 2014, then White House Cybersecurity Coordinator Michael Daniel revealed that the process considers nine criteria, including whether a vulnerability is found in core infrastructure and the likelihood that adversaries will find it. While disclosing a vulnerability might mean the U.S. forgoes "an opportunity to collect crucial intelligence that could thwart a terrorist attack," Daniel wrote, hoarding them also has risks. "Building up a huge stockpile of undisclosed vulnerabilities while leaving the internet vulnerable and the American people unprotected would not be in our national security interest."[11] In 2015, NSA Director Admiral Michael Rogers said the agency discloses 91 percent of the vulnerabilities it finds.[12]

Microsoft's Smith argued that the leaks of NSA exploits is evidence that the VEP process is broken and that the government cannot safely stockpile vulnerabilities. "An equivalent scenario with conventional weapons would be," according to Smith, "the U.S. military having some of its Tomahawk missiles stolen."[13] In response, he argues the government should no longer stockpile, sell, or exploit vulnerabilities, but should report them to vendors.

Beijing's Assertive Cyber Diplomacy

The rupture between Washington and Silicon Valley is occurring at a time when China is taking a more active role in shaping cyberspace, and Chinese firms are playing a central role in the next wave of innovation. Beijing's early cyber diplomacy efforts were essentially a defensive crouch. China worked to control the destabilizing influence of the internet and the free flow of information through domestic laws and the deployment of filtering and censorship technologies widely known as the Great Firewall. On the international level, Beijing complained about what it saw as the uneven distribution of internet resources and defended itself from Western, especially American, accusations of internet censorship.

Under President Xi Jinping, China has more actively promoted its own vision of cyberspace governance. In November 2014, China held its first World Internet Conference in Wuzhen, a historic town near Hangzhou, home to the headquarters of the Alibaba Group. The event was meant as a showcase for the Chinese internet economy. It was at the second Wuzhen conference in 2015, that President Xi delivered his comments concerning "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing."[14]

Beijing has also used trade and investment in information technology infrastructure as an economic and political tool; much of the current investment and trade occurs as part of the One Belt, One Road (OBOR) initiative, a development strategy focused on connectivity and cooperation between China and Eurasia. Official Chinese documents have also stressed the need to build an "information silk road" through cross-border optical cables and other communications trunk line networks, transcontinental submarine optical cable projects, and spatial (satellite) communication.[15]

Chinese firms have invested in nodes along the Belt and Road. China's state owned telecommunication companies are planning new operations in Africa and Southeast Asia. China Comservice, a subsidiary of China Telecom, announced the "Joint Construction of Africa's Information Superhighway between China and Africa" with investment amounting to $15 billion and a 150,000 kilometer optical cable covering 48 African countries.[16] Private companies have also been active. In 2016, Chinese telecom equipment maker ZTE agreed to take over Turkish company Netas Telekomünikasyon for up to $101.28 million in a deal that would expand its operations across key markets covered by OBOR. Alibaba executive chairman Jack Ma is an adviser to the Malaysian government on the digital economy, and Huawei, in cooperation with Telekom Malaysia, is setting up a regional data hosting center in the country.[17]

Attempts to Bridge the Gap

The Obama Administration scrambled to repair the damage with the private sector. Driving the outreach was a belief not only that cooperation between the two sides was necessary in cyberspace but also that the next wave of defense innovation would occur in the private sector, not federal labs. In the past, government research and development was the main driver of technologies critical to the second offset, such as precision-guided weapons, stealth, imaging and sensor technology, and electronic warfare. Robotics, artificial intelligence, and the other technologies that define the third offset, however, will come from the nexus of public-and private-sector research and development. As former director of the Defense Advanced Research Projects Agency Arati Prabhakar put it, the secret of success is "going to be to harness that commercial technology and to turn it into military capabilities much more powerful than anyone else."[18]

Soon after the Snowden revelations, President Obama appointed a team of lawyers and national security experts to review the balance between privacy and security as well as efforts to promote an open internet and pursue commercial interests. In December 2013, the President's Review Group on Intelligence and Communications Technologies issued 46 recommendations on how to reform surveillance, including curtailing spying on foreigners to instances "directed exclusively at protecting the national security interests of the United States and our allies." The Group also noted the importance of encryption to the economy and urged the USG not to "in any way subvert, undermine, weaken, or make vulnerable generally available commercial software."[19]

In January 2014, the White House released Presidential Policy Directive (PPD) 28 on signals intelligence activities. PPD 28 affirmed the uses of intelligence collected in bulk for only six categories of threat (espionage, terrorism, and proliferation of weapons of mass destruction, cybersecurity, attacks on U.S. or allied armed forces, and transnational criminal threats) and banned U.S. agencies from distributing information collected on foreign citizens to other foreign intelligence agencies without considering "the privacy interests of non-U.S. persons."[20] The Intelligence Community must also delete a foreigner's personal information after five years unless it is determined that the information has intelligence value. PPD 28 was meant as an olive branch to the United States' European allies, but was also important to the companies, as it relieved some of the pressure European privacy regulators were putting on U.S. companies.

Obama White House and Department of Defense (DOD) officials also made numerous trips to Silicon Valley. The President gave talks at Stanford University and SXSW, an Austin-based festival of technology, music, and media. Defense Secretary Ashton Carter made four trips to Silicon Valley in 15 months. None of his predecessors had made the trip in 20 years.[21] Carter also created new institutions to strengthen ties. The Defense Innovation Unit Experimental (DIUx) is intended to help the military better tap into commercial tech innovation through more agile contracting and procurement. While DIUx struggled at first with slow acquisition times, it has had more recent successes, investing, for example, in a startup working on small civilian radar satellites that the Pentagon hopes to use over North Korea.[22]

Secretary Carter also established in March 2016 a Defense Innovation Advisory Board, made up of leaders from technology companies outside of the traditional defense industries, to offer "advice on innovative and adaptive means to address future organizational and cultural challenges." Chaired by Alphabet Executive Chairman Eric Schmidt, the board recommended the appointment of a chief innovation officer, the creation of a center for artificial intelligence and machine learning, and embedding software development teams within key commands.[23]

Former U.S. Secretary of Defense Ashton Carter stands in front of the Facebook wall during his visit to the company headquarters in 2014. Before the visit, the Defense Secretary unveiled DOD's cyber strategy at Stanford University. (DOD/Clydell Kinchen)

What Happens Next?

Despite calling for a boycott of Apple and warning Amazon it would face antitrust investigations as a presidential candidate, Donald Trump quickly invited CEOs to a Tech Summit soon after his election in November 2016. The meeting reportedly discussed vocational education and the application of information technology (IT) to reducing government waste. In June 2017, Apple Chief Executive Officer Tim Cook and Amazon CEO Jeff Bezos were among 18 executives who attended a meeting sponsored by the newly established Office of American Innovation. The office, led by Jared Kushner, aims to modernize federal IT systems, reduce government spending on IT, and improve the cybersecurity of government networks. Secretary of Defense James Mattis has signaled that he will continue support of DIUx.

Still, the relationship, as noted above, remains contentious, and issues such as immigration and climate change continue to drive the wedge. Both sides need to be realistic about what can be achieved, so as to insulate themselves from wide swings of emotion from over exuberance to a sense of betrayal. It is important that both sides acknowledge that distrust is bound to endure for at least two reasons. First, the economic incentives for Apple, Facebook, Google, Microsoft, and others to protect the privacy of their global users and publicly oppose the USG are unlikely to change. Opportunities to work more closely with the USG will not outweigh the lure of foreign markets. Second, as noted above, the platforms of these same companies will remain the target of NSA and other intelligence agencies. Potential U.S. adversaries, along with terrorists, hackers, and criminals, use commercial software and hardware. The Trump Administration, however, has the opportunity to put the relationship back on firmer footing with actions in three areas: encryption; data localization; and reforms of the VEP.

The encryption debate is a Gordian knot, with national security policymakers avowing there is a technological fix and the tech community asserting the opposite. In July 2017, for example, Acting Assistant Attorney General for National Security Dana Boente told the Aspen Security Forum, "I'm sure we'll find some technological brilliance that will provide the necessary security but still allow the government to do it [access encrypted data]."[24] That technological solution is, however, not coming, and efforts to force exceptional access are likely to result in lengthy battles pitting civil rights organizations and tech companies against the government.

Instead of seeking backdoors, the Trump Administration can explore other avenues of access to data. Despite concerns about encrypted devices, the FBI and others now have the ability to access texts, emails, social networking sites, and other data stored in the cloud. There is also a wealth of data being created and collected by new types of sensors in our phones, cars, and household devices.[25] Prosecutors in Arkansas recently demanded, for example, the recordings of an Amazon Echo smart speaker as evidence in a murder case.

Another option is to bypass encryption by exploiting existing security flaws in software to gather data. Known as lawful hacking, this would give law enforcement agencies the ability to hack into a suspect's smartphone or computer with a court order, such as a warrant. This type of hacking is likely to be resource intensive, requiring the development and acquisition of vulnerabilities, and so should be restricted to terrorism, violent crime, large-scale narcotic trafficking, and other serious threats.[26] Germany has taken such an approach, authorizing the police to use malware in investigations.[27]

As a corollary, law enforcement and investigative agencies will have to increase their investment in technology and technical expertise. The FBI, for example, has only 39 staff members who deal with encryption and anonymization technologies (eleven of whom are agents), and only $31 million in funding for those activities.[28] Congress should also provide funding for the FBI to share its capabilities with state and local police, who do not have adequate technological resources.

A second, actionable area for cooperation is creating a framework to respond to growing international demands for access to data. China, India, Indonesia, Malaysia, Nigeria, South Korea, Russia, and Vietnam have passed or are considering regulations that would require user data to be stored locally. The push to keep data within national borders has been driven in part by widespread frustration with the time-consuming and confusing legal processes involved in acquiring data from U.S. companies, which are prohibited under the Electronic Communication Privacy Act (ECPA) from releasing users' communications to foreign governments or authorities without a warrant from a U.S. judge.

This means that if an Indian citizen, for example, uses a Microsoft messaging app to plan and execute a crime in Delhi with other Indian citizens, Microsoft cannot disclose the messages directly to the Indian authorities. Instead, the Indian police has to request assistance from DOJ to petition a U.S. judge to obtain the communications on behalf of India. This process, enabled by a mutual legal assistance treaty (MLAT), is opaque, time consuming, and challenging for foreigners unfamiliar with the U.S. justice system. An MLAT request generally takes ten months to process, and U.S. companies are often forced to choose between two countries' legal demands.

During the Obama Administration, the United States and United Kingdom negotiated an agreement that would allow U.K. law enforcement agencies to request stored data and live intercepts directly from U.S. service providers, as long as the warrants did not target U.S. citizens, legal permanent residents, or anyone physically present in the United States. The Justice Department also introduced legislation that would allow the President to negotiate agreements with other foreign countries in which U.S. firms could respond to local law enforcement demands for emails and other communications. The legislation amends ECPA and authorizes Facebook, Google, and other U.S. providers to disclose data and communication content only to foreign governments that adhere to baseline due process, human rights, and privacy standards. The Trump Administration should continue this effort and work with Congress to ensure its adoption. As the ECPA reform process progresses, the Department of Justice should

The USG will not, and should not disclose all vulnerabilities to the private sector. There are legitimate security, intelligence, and law enforcement reasons for the government to hold on to vulnerabilities, and potential U.S. adversaries will not release disclosures to the public. But officials can be more transparent about the criteria for holding on to vulnerabilities, standardize the process of evaluation, and publish an annual report on the VEP's operations.

streamline the MLAT process. There should be a standard template for MLAT requests so that foreign governments know exactly what information they must provide to expedite the process, and the forms automated and simplified.

Third, the Trump Administration could reform the VEP. The USG will not, and should not disclose all vulnerabilities to the private sector. There are legitimate security, intelligence, and law enforcement reasons for the government to hold on to vulnerabilities, and potential U.S. adversaries will not release disclosures to the public. But officials can be more transparent about the criteria for holding on to vulnerabilities, standardize the process of evaluation, and publish an annual report on the VEP's operations. The President may also want to consider an executive order that formalizes the VEP process.[29]

It will not be enough just to be active at home. Beijing may benefit from Washington's apparent turn inward to play a larger role in defining the rules of the international order in cyberspace. The preliminary U.S. position on renegotiating the North American Free Trade Agreement does include provisions to "secure commitments not to impose customs duties on digital products, prohibit forced data localization, and ban governments from mandating the review of source code."[30] The abandonment of the Trans-Pacific Partnership, however, is likely to weaken U.S. efforts to shape cyberspace for its commercial and security interests as countries look to China. In particular, the growing trend of data localization is something China may be able to exploit diplomatically and economically.

Conclusion

Without any progress on these issues, U.S. technology companies are likely to continue to try and carve out their own path. The private sector will respond to the administration with limited cooperation on information sharing, a greater focus on encryption and other technological solutions for defending their own networks, and individual deals with governments around the world to smooth access to technology.[31] Apple, for example, announced in July 2017 that it would open its first data center in China.[32]

There is, of course, a limit to how far the companies will go. Technology companies are not of one mind on all of these issues, and some firms will continue to work with the USG. Some of those who protest loudly will find areas to cooperate quietly. Perhaps most important, the USG, and DOD in particular, remains an important customer. Or as Terry Halvorsen, the former Chief Information Officer of the Pentagon, put it: "I spend $36.8 billion a year. That buys a lot of potential trust."[33] It is not in the U.S. interest, however, to see how far that trust can be stretched. Unless the two sides find some common areas of cooperation, the U.S. ability to shape cyberspace in the near term is bound to be limited. PRISM

Notes

[1] Adam Segal, *Rebuilding Trust Between Silicon Valley and Washington*, Council on Foreign Relations Special Report, January 2017, available at <https: //www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington>.

[2] Jack Stubbs and Matthias, "Ukraine scrambles to contain new cyber threat after 'NotPetya' attack," *Reuters*, July, 2017, available at <http://www.reuters.com/article/us-cyber-attack-ukraine-backdoor-idUSKBN19Q14P>.

[3] Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference, December 16, 2015, available at <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml>.

[4] "India Presses Microsoft for Windows Discount in Wake of Cyber attacks," *CNBC*, June 30, 2017, available at <http://www.cnbc.com/2017/06/30/india-presses-microsoft-for-windows-discount-in-wake-of-cyber-attacks.html>.

[5] FBI Director James Comey keynote address at the first annual Boston Conference on Cyber Security, March 8, 2017, available at <https://www.c-span.org/video/?424885-2/director-comey-remarks-cybersecurity-conference>.

[6] Mark Scott, "In Wake of Attack, U.K. Officials to Push Against Encryption Technology," *New York Times*, available at <https://www.nytimes.com/2017/03/27/technology/whatsapp-rudd-terrorists-uk-attack.html?mcubz=0>; Kieran McCarthy, "Look Who's Joined the Anti-encryption Posse: Germany, Come on Down," *The Register*, June 15, 2017, available at <https://www.theregister.co.uk/2017/06/15/germany_joins_antiencryption_posse/>.

[7] David Kravets, "Apple CEO Tim Cook blasts encryption backdoors," *ArsTechnica*, October 20, 2015, available at <https://arstechnica.com/tech-policy/2015/10/apple-ceo-tim-cook-blasts-encryption-backdoors/>.

[8] Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," February 11, 2016, available at <https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf>.

[9] "Global Government Surveillance Reform," Reform Government Surveillance, May 19, 2015, available at <https://www.reformgovernmentsurveillance.com>.

[10] Brad Smith, "The need for a Digital Geneva Convention," available at <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

[11] Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," available at <https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>.

[12] Sean Lyngass, "NSA chief says agency discloses '91 percent' of zero day bugs," *FCW*, November 9, 2015, <https://fcw.com/articles/2015/11/09/rogers-zero-days-nsa-lyngaas.aspx>.

[13] Brad Smith, "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack," available at <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#zKiyEOFe1dxIx1zB.99>.

[14] "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference," Ministry of Foreign Affairs, December 12, 2016, available at <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml>.

[15] "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," Consulate-General of the PRC in Vancouver, April 4, 2015, available at<http://vancouver.china-consulate.org/eng/topic/obor/>.

[16] For more information please reference <http://www.ey.com/Publication/vwLUAssets/ey-china-go-abroad-4th-issue-2016-en/$FILE/ey-china-go-abroad-4th-issue-2016-en.pdf>.

[17] Lokman Mansor, "Jack Ma is Now an Adviser to Malaysian Government on Digital Economy," *New Strait Times*, November 4, 2016, available at <http://www.nst.com.my/news/2016/11/185930/jack-ma-now-adviser-malaysian-govt-digital-economy>.

[18] Mohana Ravindranath, "DOD's Current InfoSec Strategy Is 'Patch and Pray,'" Nextgov, October 1, 2015, available at <http://www.defenseone.com/ideas/2015/10 /dods-current-infosec-strategy-patch-and-pray/122457/?oref=d-river>.

[19] White House, Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, available at <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

[20] White House, Presidential Policy Directive—Signals Intelligence Activities, January 17, 2014, available at <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

[21] Henny Sender, "U.S. Defense: Losing its edge in technology?" *Financial Times*, September 4, 2016, available at <https://www.ft.com/content/a7203ec2-6ea4-11e6-9ac1-1055824ca907>.

[22] Dan Lamothe, "Pentagon Chief Overhauls Silicon Valley Office, Will Open Similar Unit in Boston," *Washington Post*, May 11, 2016, available at <https://www.washingtonpost.com/news/checkpoint/wp/2016/05/11/pentagon-chief-overhauls-silicon-valley-office-will-open-similar-unit-in-boston/?tid=a_inl-amp&utm_term=.669353214d20>; David Sanger and William Broad, "Tiny Satellites From Silicon Valley May Help Track North Korea Missiles," *New York Times*, July 6, 2017, available at <https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html>.

[23] U.S. Department of Defense, "Pentagon to Establish Defense Innovation Advisory Board," March 2, 2016, available at <https://www.defense.gov/News/Article/Article/684366/pentagon-to-establish-defense-innovation-advisory-board/>; Aaron Mehta, "Defense Innovation Board Lays Out First Concepts," *DefenseNews*, October 5, 2016, available at <http://www.defensenews.com/articles/defense-innovation-board-lays-out-first-concepts>.

[24] Morning Cybersecurity, July 24, 2017, available at <http://www.politico.com/tip-sheets/morning-cybersecurity/2017/07/24/will-the-us-follow-europe-on-encryption-221486>.

[25] "Don't Panic Making Progress on the 'Going Dark' Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, available at <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>.

[26] Susan Hennessey, "Lawful Hacking and the Case for a Strategic Approach to "Going Dark," Brookings, October 7, 2016, available at <https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/>.

[27] Joseph Cox, "Germany Just Gave Cops More Hacking Powers to Get Around Encryption," Motherboard, June 22, 2017, available at <https://motherboard.vice.com/en_us/article/gyp7em/germany-just-gave-cops-more-hacking-powers-to-get-around-encryption>.

[28] Robyn Greene, "Unbounded and Unpredictable," Open Technology Institute, New America, August 22, 2016, available at <https://www.newamerica.org/oti/blog/unbounded-and-unpredictable>.

[29] Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," Belfer Center for Science and International Affairs, June 2016, available at <http://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf>.

[30] U.S. Trade Representative, Summary of the Objectives for the NAFTA Renegotiation, July 17, 2017, available at <https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf>.

[31] Segal, *Rebuilding Trust*.

[32] Paul Mozur, "Apple Opening Data Center in China to Comply With Cybersecurity Law," *New York Times*, July 12, 2017, available at <https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html?mcubz=0>.

[33] Sara Sorcher, "Pentagon's Top IT Official: My Money Buys Silicon Valley's Trust," Passcode (blog), *Christian Science Monitor*, October 29, 2015, available at <http://www.csmonitor.com/World/Passcode/2015/1029/Pentagon-s-top-IT-official-My-money-buys-Silicon-Valley-s-trust>.

A satellite image from September 7, 2017 shows Hurricane Irma (center) and Hurricane Jose (right) in the Atlantic Ocean and Hurricane Katia in the Gulf of Mexico. (U.S. Navy)

Battlefield Geometry in our Digital Age

From Flash to Bang in 22 Milliseconds

By Robert Allardice and George Topic

This year has been tough for cybersecurity programs. Every month in the first six months of 2017, the world experienced a major cyber event. Open-source attacks included attacks on critical infrastructure, banks, intelligence services, and significant commercial and government entities. Indeed, reflecting on the scope and depth of most publically acknowledged compromises, uncovers the reality of the tremendous and growing risks the country faces nearly two decades into the 21st century. Everything seems to have changed. Virtually every organization within the Department of Defense (DOD) has, sometimes reluctantly, come to embrace digital age technology, to the point that they are completely dependent on it. The result is a shocking degree of paralysis when our access to the services we now rely upon is disrupted.

The paradox DOD faces is that the asymmetric advantage delivered by application of digital age tools can easily become an asymmetric disadvantage. That is, the very advantage gained through the speed, connectivity, and non-linear impacts delivered by leveraging the benefits of cyberspace, may be disrupted or denied with counter levers delivered by adversaries through the same medium. Is the United States, and more specifically DOD, prepared to deal with this?

This article describes a simple model that not only will give military commanders the highest probability of mission assurance but is applicable for the 99 percent who have become dependent upon cyberspace and digital age tools. Unfortunately, the 800-pound gorilla in almost every organization is: "What do we do if the systems delivering the knowledge and data are corrupted, exfiltrated, or denied?" Cyberattacks occur with little or no warning—from "flash to bang" in 22 milliseconds, or sooner—and victims often are unaware of an intrusion until significant quantities of data are impacted. A set of precepts is also proposed that can assist leaders in developing, arranging, and exercising the people, processes, and tools that will optimize capabilities and give commanders the highest probability of mission assurance on the digital battlefield. As a final point, a series of general recommendations is provided for consideration by leaders, managers, and policy makers at all levels to help manage the manifest challenges before us.

Lieutenant General (ret.) Robert Allardice previously served as Vice Commander, U.S. Air Mobility Command. He is a senior civilian mentor for Joint Force Development (J7) and a Senior Fellow at National Defense University. Mr. George Topic is Vice Director, Center for Joint and Strategic Logistics at Ft. McNair.

It is important for leaders at all levels to truly understand the nature of what is needed and to not mistake activity for progress or, even worse, victory. One of the most pernicious and dangerous responses to questions about cyber defense issues is, "We have already got that covered."

The New Battlefield

The digital age has changed battlefield geometry. In fact, the changes to warfare during the past several decades have been so profound that many central tenets of military theory enduring for generations or even millennia no longer apply—in some cases they are actually dangerous. Perhaps the best illustration of this point is the recognition that the battlefield is no longer physically bound or adequately described within the narrow frame of traditional kinetic effects. The speed, connectivity, and non-linear nature of the environment in which warfighters must operate, fundamentally changes how one must think about objectives and the threats we face. The geometry that has been used throughout history may no longer apply. Not only are physical boundaries less relevant, but the many dimensions or domains of warfare are also more closely integrated than ever before. Failure in any facet may compromise the entire mission and put the force and the nation at risk.

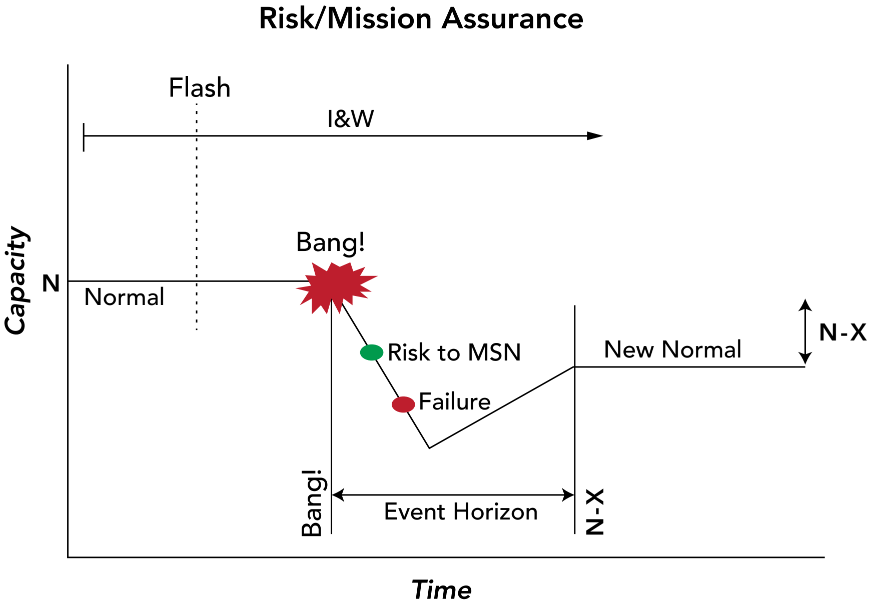
The Cyber Mission Assurance Model depicted in Figure 1, is derived from a RAND Corporation study and is intended to help leaders think through the challenges they face.[1] It can also provide the intellectual framework to develop the ability to survive and operate in a cyber challenging environment. The following paragraphs give an in-depth presentation of the model.

Ability to Survive and Operate: A linear Model to Assess the Current Challenge

First, a description of the model itself. Note, the vertical axis represents capacity and the horizontal axis represents time. Capacity, or organizational output ("N"), represents a notional, normal, sustainable level. At some point following along the timeline, an event occurs, labeled "bang." This is often that painfully obvious moment of an attack, intrusion, or other negative effect, occurring and impacting an organization. Generally an event is preceded by a "flash," an indication that the event is imminent or underway. Once an event occurs, the model shows a decrease in capacity at a given slope. At some point capacity is diminished to a level that puts the mission at risk. If capacity continues to decrease, at some discernable point, mission failure is imminent. Of course, as the organization reacts to the event, mitigation measures often begin to restore capacity at a given rate to a new

The geometry that has been used throughout history may no longer apply. Not only are physical boundaries less relevant, but the many dimensions or domains of warfare are also more closely integrated than ever before. Failure in any facet may compromise the entire mission and put the force and the nation at risk.

FIGURE 1: Cyber Mission Assurance Model.



"normal" labeled "N–X."[2] Each event has a life cycle labeled here as the event horizon. Finally, preceding an event, and throughout the event horizon, indications and warnings (I&W) provide data to inform decisionmakers at a level of detail that they are able to visualize the battlespace.[3]

Many immediately grasp the application of the model in a general sense, and more specifically when applied to the multi-domain problems presented by the modern battlefield. In basic terms, one can see how this simplistic model illustrates what most encounter as missions are accomplished. Consider capacity; most organizations have a set of capabilities that produce some type of capacity. This could be a product or a level of service. In the case of military organizations, at the highest level, the product is ultimately combat capacity. Organizations within DOD and other government agencies, usually spend a great deal of time measuring their ability to generate capacity. During peacetime, the military maintains a fairly consistent capacity to deter war and to prosecute a steady state-level of small conflicts. During times of total war or significant increase in demand, the nation mobilizes to a higher level.

Organizations performing at normal capacity often have I&W available to them essentially to identify threats to their ability to accomplish their mission with sufficient time to begin mitigating measures. Threats to the mission are often assessed from a risk perspective— i.e. how much risk does a particular threat present to the mission? For example, historical data shows significant weather events during the fall season so airports on the East Coast will look for indications of tropical storms. At some point, a hurricane may actually develop and the system will produce warnings of the direction, strength, speed, and potential impact of the storm. If a hurricane poses a significant risk to operations, airport leadership will order evacuations or take other mitigating actions. Looking at the model, notification of an imminent hurricane would be a flash.

When bang actually occurs with an impact that degrades mission performance (reduced capacity), the effect may be sudden or gradual reflected by the slope of the line. A catastrophic event can cause a total collapse which would be a near vertical slope, while a shallow slope would indicate a gradual decrease in capacity. As event impact increases or endures, at some point the mission of the organization is at risk. If the event continues unmitigated, the organization will eventually become crippled past the point of meeting mission needs or the production demands. This point is called mission failure. In most cases, some form of recovery from the event mitigates the negative impact causing a positive rebound to the curve. Again, slope matters. A rapid recovery is indicated by a steeper climb and decreases the event horizon time.

Broadly speaking, the role of the decisionmaker throughout the event consists of; setting the conditions to understand the I&W prior to the event occurring, ensuring the right processes and plans are in place to implement mitigation measures once flash has occurred, ordering mitigation measures when appropriate, and once bang has occurred, initiating reconstitution measures. Note using the hurricane example, many military organizations, particularly those that have suffered through a catastrophic hurricane, put considerable energy into planning and exercising in anticipation of future hurricane events. They have learned the value of actions left of flash, and sadly in some cases, the consequences of inattention left of flash.

Leaders should use variations of this model to think through and explain almost any event that impacts mission, not simply cyberattacks. Leaders want to perform at a designated capacity and to recognize events and risks with sufficient time to mitigate negative impacts. Generally, an organization's objective is mission assurance. All of the services, agencies, and commands within DOD have invested, and will continue to invest, in multiple systems to ensure they are able to accomplish their mission.

Unfortunately, application of this model through a multi-domain or cyber lens exposes complexities and risks that should concern all leaders. The interdependence of the cyber domain with all other domains presents significant risk profiles, and suggests the need to think through this concept of mission assurance from a different perspective than the current and historical "three-dimensional warfare." Threat vectors are not just from air, land, sea, or space, but can come from any direction through the internet; in the cyber domain distance is generally not a factor or limitation. Nefarious actors acting either under the sanction of a nation-state or, as stand-alone agents, can introduce risk to systems with devastating consequences. Another particularly vexing aspect of cyberattacks is trying to determine if one is at war at all. At what point is a cyberattack considered an act of war?

Now think through the model with the lens of a mission under threat of a cyberattack. Operating at

The interdependence of the cyber domain with all other domains presents significant risk profiles, and suggests the need to think through this concept of mission assurance from a different perspective than the current and historical "three-dimensional warfare."

normal capacity, leaders should understand specifically how dependent their mission is on cyber systems, just as they understand mission dependency on aircraft, ships, infantry, etc. The model demands a level of knowledge about systems in order to make informed decisions based on specific I&W. Success after bang rests largely on planning and exercising in a realistic way. Experience in the past has indicated a lack of realistic planning and a nearly wholesale propensity to ignore realistic exercises. In fact, most commonly in exercises, cyber events are either treated as "stand-alone" (non-dependent) or a "white card" issue explained away without demonstrating how the unit will actually accomplish the mission.

The temporal impact of events complicates everything. In this battlespace, events move from flash to bang at extreme velocity and can deliver profound and even lethal effects before the victim is even aware of the threat. We literally go from flash to bang instantaneously and may be on a significant slope of reduced capacity moving towards mission failure unknowingly.

Moreover, the impact from these events can last for years, undoing projects, programs, and relationships that took far more years to develop. In the well-documented and widely known STUXNET attack on Iranian centrifuges, while it is hard to accurately assess the actual impact, it is clear that it was significant. Beyond the physical destruction of a major portion of Iran's centrifuge inventory, a major clean-up and security review of their programs was also necessary for them to continue the programs with confidence that their equipment was not compromised. The recent cyberattack in the Ukraine involving Petya malware, not only significantly affected government and public service activities, but spread to many other nations, commercial firms, and other entities across Europe, and around the world. While this could have been a simple criminal ransomware attack, there is speculation that it could also have been politically motivated or an act of hostility by an adversarial nation. It is the uncertainty that such attacks foster that causes the most damage; in some cases, prevention or remediation causes processes to be slowed significantly, adversely affecting major decisions and operations.

Success in the digital age fight demands considering the implications within the context of this model and taking large steps left of flash to understand and mitigate potential impacts of cyber threats. Additionally, the integration of cyber system experts and operational system experts must be sufficient to rapidly comprehend when bang occurs, and the slope of the line. Moreover they must have appropriate resources and authorities to take immediate mitigating steps.

This model can be applied at strategic, operational, or tactical levels. While the implications are different for each, the application is appropriate at each level. Though this article focusses on DOD, when applying it at a strategic level, it is relevant for the entire national security enterprise. Let the reader also note, that in the deeply intertwined world of international and multinational relationships, systems, and processes, even trying to develop national solutions may not be adequate. As pointed out above with the Ukrainian Petya malware attack, cyber operations are difficult to contain within a geographic space. Electrons do not recognize international borders. Consequently, cooperation among nations plays a part in both prevention and remediation. Similarly, attacks and intrusions in the commercial sector can find their way into DOD systems.

Precepts of Digital Mission Assurance

So far, this article paints a bleak picture. Rational and reasonable reliance on digital age tools and processes has produced quantum improvements in the United States' military capabilities, and absolutely extends our asymmetrical advantages.

However, it also presents asymmetrical vulnerabilities when viewed from the context of the cyber threat. One may find it easier to ignore the problem than to invest what is necessary to deal effectively with this Rubik's Cube. Unfortunately, while there has been a great deal of discussion about the impact of cyber events, at lower organizational levels and broadly throughout DOD, there seems to be some degree of paralysis in determining what an individual commander or individual organization should be doing today to achieve a high-degree of mission assurance.

While the challenges in the cyber domain can seem overwhelming and cause uncertainty in leaders about what to do or even how to think about the problem, there are things every organization can, and should, be doing. To be clear, cyber defense in and of itself is not sufficient; it is truly the clearest expression of a 21st century Maginot Line imaginable. In fact, it is the assertion, and a central theme of this article, that one cannot defend against the threat completely, that one must structure a methodology to accomplish the mission within the realities of the new battlefield geometry. If it is not obvious yet, let it be clearly stated: an organization cannot wait for flash or bang. The focus must be on the need for actions left of flash.

A set of precepts has been developed for organizations, commanders, and leaders at all levels that will hopefully assist in framing how to prepare for, and deal with, the challenges of offering capacity and performing missions. The five precepts—hygiene, redundancy, alternative practices, passive defense, and active defense—emerged from observations and experiences working with organizations (particularly in the joint world of the U.S. military) that, are struggling to discover pathways to accomplishing their missions in light of the current and anticipated threat streams. There is nothing magic or ironclad about them either in phraseology or content. The precepts are not a list of independent, progressive, actions; rather, they are intended as a framework to apply simultaneously at various degrees depending on the current environment and understanding of the problem. Each of the precepts are described on an individual level and then finally described holistically in conjunction with the model in order to offer recommendations for the road ahead.

The five precepts—hygiene, redundancy, alternative practices, passive defense, and active defense—emerged from observations and experiences working with organizations (particularly in the joint world of the U.S. military) that, are struggling to discover pathways to accomplishing their missions in light of the current and anticipated threat streams.

Hygiene

Follow the basic cybersecurity principles and guidance. While this precept is obvious, it continues to be one of the most challenging for most organizations. To ensure mission success, every level within every organization must comply with basic blocking and tackling efforts such as virus scanners, the use of credentials, and password discipline. These are the typical things cybersecurity experts indicate are critical to insure a minimum level of mission assurance. In reference to the model, hygiene consists of the individual and collective actions that prevent an easy bang for/from the enemy. Interestingly, there seems to be a persistent, misguided belief that imposing a set of rules by itself will accomplish cybersecurity. This simply is not true and is a particularly dangerous fallacy. In an organization of 100 people, it only takes one person to have a minor lapse in judgment or attention to compromise the whole system. In the cyberattack known as Buckshot Yankee, a flash drive inserted into a single laptop computer introduced a virus that took at least 14 months to clean out, and estimates of the damage range as high as $5.1 billion. Despite significant efforts to mandate rules, experts indicate a substantial number of organizations continue to be compromised by 10–20 percent of their employees who do not comply. Relying solely on hygiene is insufficient.

Redundancy

Aggressively and continuously pursue multiple pathways to accomplish the mission if a specific system is compromised. The concept of having redundant systems seems straightforward—if a system is compromised or attacked we need to have the ability to jump to another system that will accomplish the same objectives. This can be very expensive, but it is effective. The common mistake many organizations make is to assume they must have redundancy within their own organization; redundancy can be seen from a much more holistic perspective. For example, DOD may find it must rely on the commercial sector for redundant systems to accomplish some objectives if its systems come under attack. The key is to know which systems can be accessible that present redundant capabilities and the impact of moving to those systems. Experience has shown that organizations often rely on a system they see as redundant, and yet, they have not exercised or practiced it. When they eventually do exercise this perceived redundant system, they realize there are significant unintended consequences, or it does not provide the required capability.

Alternative Practices

Develop a non-cyber dependent backup process. The most common practice heard about when participating in exercises outside of the actual cyber force, is reliance on alternative practices. For example, when asked what happens if the system was attacked someone will say "we go to alternative, manual, practices." One hundred percent of the time when asked if an organization ever completely exercises the alternative practice to accomplish their mission, the answer has been "no." For some that have actually tried a degree of alternative practice, they have found many unintended consequences for other organizations within the enterprise. The best way to achieve success using alternative practices is to exercise them completely and thoroughly on a regular basis. The combination of redundancy and alternative practices should provide the basis for a "thin line" that can be operated and defended to provide some degree

One hundred percent of the time when asked if an organization ever completely exercises the alternative practice to accomplish their mission, the answer has been "no."

of mission assurance even under the most severe level of attack.

Passive Defense and Active Defense

Try to know as much as you can about the enemy and take specific, measured, and thoroughly coordinated steps with respect to the enemy. These two precepts are combined because of their common foundation. For both active and passive defense, there is a level of understanding and knowledge of the enemy to develop. Digital age battlefield geometry transcends traditional lines of communication, placing a new demand signal for this in-depth comprehension of the enemy beyond traditional boundaries. Defense is largely dependent on understanding the true environment, knowing the enemy and its intent, capabilities, and vulnerabilities. Behind every attack or threat there is ultimately a human. That human has a capability, a purpose, and an intent. That human may be acting as an individual actor, a terrorist's activity, or as part of a sanctioned government. Defense is not about building a modern Maginot Line, nor is this about handing the defense requirement to U.S. Cyber Command. These precepts are based on the fundamental obligation of every organization to take full ownership of the mission's success, a subset of which is to own the defense problem. Then, in conjunction with the experts, construct a strategy to raise the confidence to deliver mission assurance.

Passive Defense

Passive defense is to develop the understanding of the new battlefield geometry, the environment within which your organization must perform, the specific threats to the mission and, in conjunction with mission partners and cyber experts, construct the actions left of "flash" required to *block* the success of the enemy.

Active Defense.

Active defense is to develop the understanding of the new battlefield geometry, the environment within which your organization must perform, the specific threats to the mission and, in conjunction with mission partners and cyber experts, construct the actions left of "flash" required to *neutralize* enemy capability before it can be brought to bear. In most cases, for military application this includes inputs to the joint targeting process. This can be a critical point. Historically, the logistics community would not consider that they had reason to have input to joint targeting. However, within the context of the digital age battlefield, to assure mission success, the joint logistics enterprise should identify multiple threats to dependent systems which require active defense actions left of "flash." This will require a nontraditional analysis of the enemy and assessment based on comprehension of the battlespace.

It is often reported that organizations such as U.S. Transportation Command (USTRANSCOM), have as many as 200,000 intrusion attempts on any given day. The vast majority of those attempts are things that normal hygiene can mitigate. Those normal hygiene actions must continue. Simultaneously, efforts to defend against threat vectors using passive and active measures within the definitions offered above can substantially raise mission assurance confidence. Finally, knowing that defensive measures can fall short, aggressive efforts to expand access to redundant capability while developing and exercising realistic alternative practices should be a high-priority. It is incumbent on every functional and mission commander to understand the new battlefield geometry and the mission assurance mitigation measures that can address the thrust of the mission measures that lead to success.

Recommendations

Actions Left of Flash

The focus must be on the actions left of flash. While there are actions that are more applicable at some levels, or in some kinds of organizations than others, there are also actions that are universal. For example, undertaking a concerted effort to seriously exercise, think through, and rehearse a left of the flash event, can be done at any level. Experience shows that as more organizations (and leaders) exercise, think through, and rehearse left of the flash, comprehension rises, along with a recognition that success does not emerge in a vacuum. There are authorities senior government officials must grant, well left of flash, to put the right processes in place to execute the steps necessary to mitigate risk once I&W exceed the threshold of tolerance.

Enterprise Perspective

There are a number of other actions that leaders at all levels can take to reduce risk and improve resilience. The basic blocking and tackling that military organizations do routinely needs to be considered in the context of cyber threats to mission assurance. Understanding and carefully assessing not only internal processes, but how other organizations are affected by yours, is also universally important. As mentioned earlier, the impact of shifting to an alternative system may have a significant impact on others. Decisions made at a tactical level might in fact render moot the actions of a major organization or compromise a major mission set.

Last Known Good

Being able to reliably identify when the "last known good," or clean data set was available, is a key part of the mitigation and remediation of effects. Once again, this is a skill that is not easily or often practiced. Clearly the timeframes required are dependent on the missions being performed. Closely related to this is the delicate skill of looking for and assessing I&W. In some cases, oversensitivity, and attendant overcompensation, might be as damaging as the consequences of an attack.

National Security Strategy for the Digital Age

The language used in this article is specific to DOD, however, the understanding of the battlefield geometry makes it clear to us that any fight in the digital age transcends the ability of DOD to fully defend the nation. This new geometry requires a national security strategy that fully comprehends the thought, authorities, and cooperation within the government, through the interagency process, that can establish the thresholds and actions required to be prepared. Once enemy intentions become imminent, it will be too late. Flash to bang happens nearly instantaneously. Additionally, modern geopolitical circumstances require thinking and action well beyond the whole-of-government and even whole-of-nation, to include partners and allies in developing a comprehensive and aggressive digital age security strategy.

Comprehensive Approach

These issues apply across multiple, or even most, government agencies and deeply into the commercial sector where the ability to direct and control actions is limited. DOD must double down on efforts to include the commercial sector as equal partners in the application of the precepts described in this paper. This thinking becomes even more important when we consider that many aspects of the defense mission are wholly reliant on the performance of the commercial sector. The Commander, USTRANSCOM testified that 90 percent of his "traffic flows on unclassified networks to and from commercial providers."[4] Additionally, a great deal of the logistics supply chain relies heavily on the commercial sector, both domestically and internationally.

Manhattan Project

Finally, we recommend the admittedly unlikely, even glib possibility of using a "Manhattan Project" approach to making the kind of progress everyone knows is needed to optimize security in the volatile and uncertain world around and before us. It is our contention that we are not preparing adequately for the wars we are most likely to fight in the years ahead—we are not only risking our competitive advantage with near-peer competitors, but making it possible even for much less capable states and other entities to harm us. The nature of such an effort is well beyond the scope of this piece, but it seems clear that such an effort would be a worthwhile investment.

Conclusion

While trying to develop cybersecurity or mission assurance solutions and recommendations, we must acknowledge that there are no absolute or permanent solutions. There is no endstate, victory or "mission accomplished." In the same vein, any recommendations are at best guidelines and suggestions that individual leaders need to tailor to their mission, organizational needs, and resources. Inevitably, there are trade-offs and the task at hand is to optimize your outcome with the capabilities you have available. In an environment where it is difficult or virtually impossible to anticipate some threats, it is likewise a challenge to decide how to prioritize your efforts. In a large and resource-constrained bureaucracy such as DOD, it is tough to make a case for investing to protect against threats you cannot see or describe—only postulate vaguely about dire impacts. Similarly, trying to discern how much effort is needed is also vexing—and an area where continual reassessment is crucial.

It is important for leaders at all levels to make sure we truly understand the nature of what we need to do and to not mistake levels of activity for progress or even worse, victory. We have entered an age where eternal vigilance is required and we are never going to be able to claim victory. On the other hand, it will be quite obvious if we are defeated, and we might not even know that we have been attacked. One of the keys to minimizing our risk is to ensure that we are all aware of the panoply of efforts, initiatives, projects, programs, contracts, proposals, organizations, etc. that are all working on some part of building cyber defense capabilities. As noted above (and worth repeating), "we have already got that covered," is one of the most pernicious and dangerous responses to questions about cyber defense issues. It is our experience that the opposite is often true, so we encourage leaders at all levels to ask more questions and examine any such claims from a holistic or enterprise perspective.

On the battlefield of the digital age, knowledge is king! Protecting knowledge is an objective as old as warfare itself. When we think of actions left of the flash, we recognize the imperative of maintaining a pure/reliable knowledge base. Therefore, it is strongly recommended that leaders pursue a high degree of confidence that on any given day they have a pure knowledge base backed up, secured, and available to the decisionmakers that need it. This is often referred to as the last known good; unfortunately for many organizations it is actually the "last good hope." That is unacceptable. PRISM

Notes

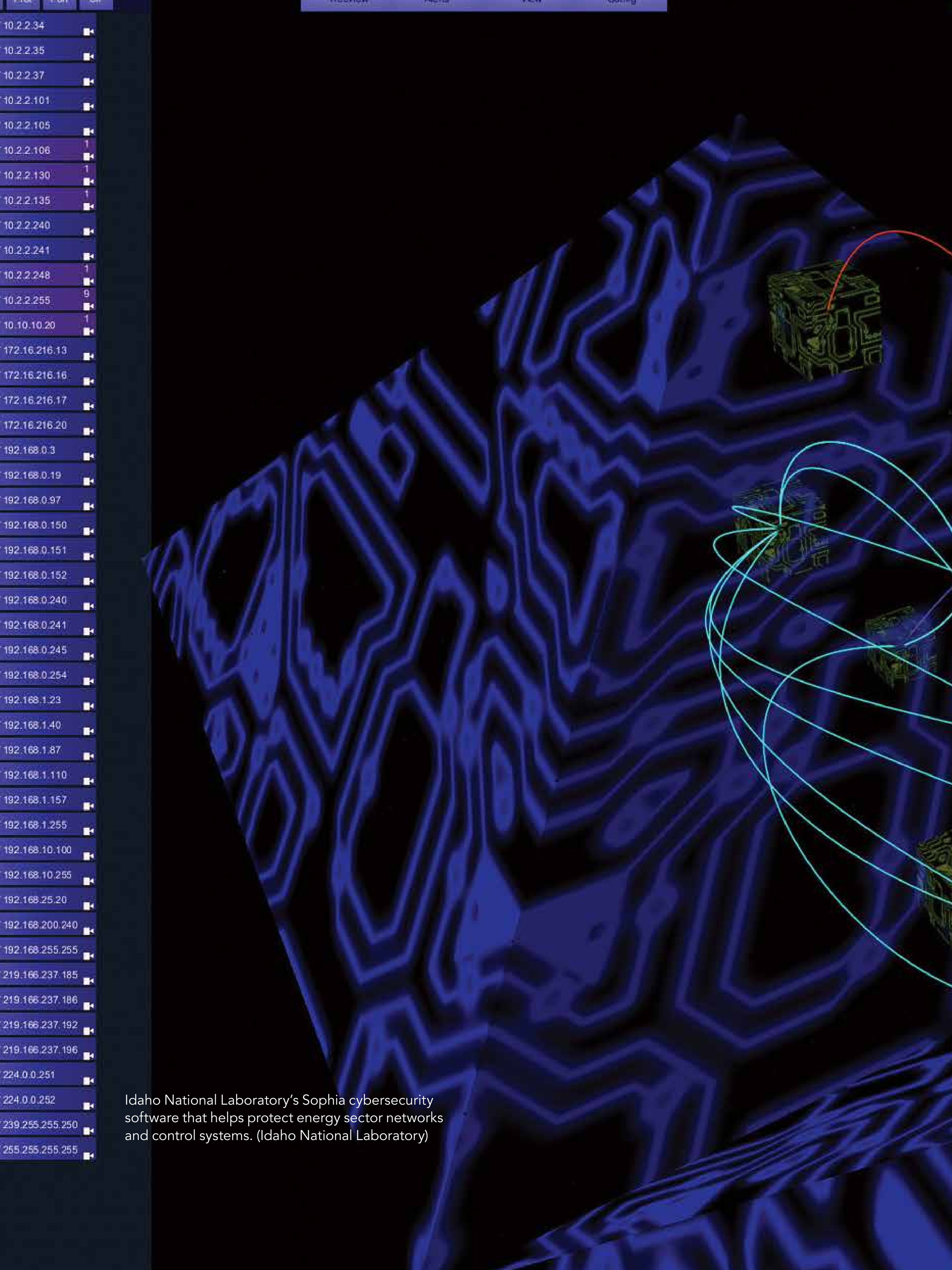
[1] Don Snyder, George Hart, Kristin Lynch, John Drew, "Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts," (Santa Monica, CA: RAND Corporation, 2015), available at <https://www.rand.org/pubs/research_reports/RR620.html>.

[2] Obviously, this could be "N+X," but not a normal result within desirable event horizons.

[3] That is the "hope" of I&W! Decisionmakers often do, and should, challenge the I&W process to ask, "Does our current I&W provide sufficient insight to accurately visualize the battle space?"

[4] *National Defense Authorization Act for Fiscal Year 2017 and Oversight of Previously Authorized Programs:*

Hearing on the U.S. Transportation Command Fiscal Year 2017 Readiness Posture, Before the House Committee on Armed Services Subcommittee on Readiness, 114th Cong., 109 (2016) Statement of General Darren W. McDew, USAF, Commander, United States Transportation Command.



Idaho National Laboratory's Sophia cybersecurity software that helps protect energy sector networks and control systems. (Idaho National Laboratory)

Cyber Gray Space Deterrence

By Richard Andres

During the past few years, adversaries of the United States have begun to use their militaries to test U.S. resolve through innovative methods designed to bypass deterrent threats and avoid direct challenges.[1] These "gray space campaigns" are specifically designed to allow adversaries to achieve their goals without triggering escalation by making retaliation difficult. China demonstrated this with its attempt to seize control of the South China Sea through its island building program, as did Russia with its effort to foment insurgency in eastern Ukraine through the use of "little green men."

Cyberattacks often are less flamboyant than the physical campaigns in the South China Sea or Eastern Ukraine, but they may cause more damage to U.S. economic and national security interests. Administration officials, for example, have estimated that China's intellectual property (IP) theft program costs the U.S. economy billions of dollars each year and, despite repeated threats from the United States, the program has persisted for more than a decade. Similarly, despite public threats by the U.S. President and leaders of allied European nations, Russia's cyber-based psychological-political campaign may be increasing in magnitude.

Virtually nothing has been done to increase the credibility of U.S. cyber deterrent threats despite widespread recognition across U.S. policy channels of the potential for cyberattacks to undermine U.S. economic and military security. Reports and strategies have been worried over but then ignored, and draft legislation has repeatedly foundered in Congress. Other than bluster, the only tangible steps the U.S. Government has taken to deter cyberattacks by foreign states has been to indict select soldiers and civilians who launched them.

When asked why the United States has been unable and unwilling to deter cyberattacks, policymakers generally provide two explanations—attribution and fear. As former Director of National Intelligence James Clapper related in his recent testimony before the U.S. Senate:[2]

> *We'll never be in a position to launch a counter attack even if we can quickly and accurately attribute who attacked us … and we're always going to doubt our ability to withstand counter retaliation.*

Dr. Richard Andres is a professor of national strategy at the National Defense University's National War College. Dr. Andres was the 2017 Scholar in Residence at the U.S. National Security Agency and a Special Advisor to the Secretary of the U.S. Air Force. The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy opinion of DOD, or any agency of the U.S. Government. Any appearance of DOD visual information for reference does not imply or constitute DOD endorsement of this work.

Both explanations accurately describe parts of the problem, yet neither offer a satisfying explanation. Although attribution can be difficult, in each of the headline grabbing cases cited earlier the identity of the attacker was known and the attacking government was subjected to diplomatic demarches. Furthermore, while it is true that the United States is more vulnerable to attacks than some of its opponents, it is also the case that the United States arguably has escalation dominance. It would not, for instance, be a great innovation for the United States to threaten economic sanctions against a state attacking through cyberspace. Thus, unless U.S. policymakers choose to restrict their deterrent threats and escalation paths strictly to cyberspace, it is not clear why cyber vulnerabilities should deter our nation from responding to attacks.

The fundamental problem the United States faces in regard to cyber deterrence is that its adversaries calculate that the benefits of their attacks exceed the risks of U.S. retaliation. This perverse incentive exists because the United States has chosen not to make strong enough threats or to back them with the actions that would lead potential attackers to believe the threats are credible. Because the United States almost certainly has the capability to make and back such threats, it has become relatively common to argue that the United States is self-deterred. However, this argument offers little new insight in that all deterrence is *self-deterrence*. To say the United States is self-deterred is merely to say its adversaries have found ways to convince it not to attempt to deter attacks.

A more useful way to frame the problem of U.S. self-deterrence is to think in terms of the specific actions America's adversaries are taking to encourage self-deterrence. The following sections explore the specific benefits adversaries gain from attacking the United States in and through cyberspace and some of the means they use to undermine U.S. deterrence.

The Benefits States Receive from Cyberattacks

During the past three decades, like many other countries, the United States connected virtually everything related to its economy and national security to computer networks and then failed to adequately defend those networks. These actions (or inactions) have created lucrative targets. The value of what cyberattackers can now obtain arguably rivals what, in previous eras, could only have been obtained through territorial conquest. States have discovered they can profit from cyberspace attacks through economic and state espionage, sabotage, and psychological operations.

Economic Espionage

Economic espionage is not new, but a number of developments have increased the importance of this type of vulnerability. First, the overall commercial value of secret information has increased in recent years. In the 1970s, for example, around 80 percent of the value of most U.S. corporations was stored in brick and mortar assets with the remainder contained in intangibles such as trade secrets and intellectual property. Today, roughly 20 percent of the value of most U.S. businesses resides in physical assets and 80 percent in information assets. A number of states use their intelligence agencies to loot their adversaries' businesses, but none come close to China either in terms of volume of commercial secrets taken or its ability to disseminate stolen intellectual property (IP) to its own commercial firms. The profit China derives from stolen commercial secrets is so great that it likely accounts for a large portion of China's often touted miraculous economic growth.

State Espionage

Like commercial espionage, traditional state espionage has also benefited greatly from cyber tools. With most state secrets now online and often lightly defended, the ability to hack secure government systems allows adversary states to garner information thousands of times more efficiently than in the past. Moreover, in the information age, the value of those secrets is often greater than in the past. This is particularly true of intelligence regarding military affairs in as much as modern military assets are generally controlled via computer chips and networks. Whereas, in the past, espionage allowed spies to learn about the location and behavior of an opponent's assets, in the current era, stolen encryption keys and related security protocols have the potential to allow their possessor to disable, destroy, or even control an adversary's hardware from a computer terminal thousands of miles from the front line. Thus, nations sometimes gain extraordinary benefits from their espionage programs.

Sabatoge

Military and civilian critical infrastructure in most industrial countries is now attached to digital networks. The vulnerability of these assets to cyberattack provides significant incentives for nations to hack them, and both commercial enterprises and military organizations regularly complain that they have discovered adversary state-originating malware on their systems. In some cases, such as Iran's attack on Saudi Aramco, U.S. banks, and a U.S. dam (2011–13), the attacks involved both gaining access to a system and doing damage.[3] However, it is more common for states to deploy malware designed to gain access to targeted systems in order to hold it at risk against potential future contingencies.[4] These hacks have the potential to do damage on par with nuclear weapons. An attack that took down the U.S. electrical grid for an extended period of time, for example, could lead to millions of deaths through starvation and related causes.[5] This ability to hold civilian and military infrastructure at risk provides a cheap substitute for conventional power projection armaments. Moreover, as the former Director of National Intelligence's comments suggest, such capabilities do not have to be executed to provide their holders with substantial coercive bargaining power.

Pyschological Operations

The first major psychological cyber operations were conducted by the United States against a range of autocratic allies and adversaries. In 2010, then Secretary of State Hillary Clinton described her intent to oppose autocracies' ability to restrict information within their borders with the intent of furthering democracy.[6] Russian and Chinese leaders believed Clinton's main goal was to foment regime change in their nations and they repeatedly attributed the rebellions associated with the Arab Spring to this policy. China responded with the internal information control and suppression programs associated with the so called Great Firewall of China. Russia, which was less concerned than China about internal stability, retaliated by developing an outward facing cyber-psychological-political capability that it used to delegitimize its opponents' governments and foment mistrust in its adversary alliances. Russia appears to receive substantial security benefits from its cyber-psychological programs.

American Reticence to Threaten Retaliation

Given the benefit various adversaries receive from their cyber programs, it is apparent that, in some cases, the United States would have to be willing to threaten substantial costs to force attackers to abandon their operations. The problem is not one of capability for the United States—it has the resources and ability to impose such costs. For example, even if China's economy gains a great deal from IP theft, China almost certainly depends even more on trade with the United States. Russia undoubtedly values what its psychological operations are doing to weaken the West, but Moscow probably is even more afraid of the types of psychological operations and economic sanctions the United States could impose on Russia should it chose to expend the resources.

Rather, the fundamental problem is that U.S. policymakers are unwilling to pay the costs. From the perspective of traditional deterrence theory, America's reluctance to seriously attempt to deter cyberattacks is puzzling. If the cost of inaction is as high as U.S. policymakers claim to believe, then why do they consistently fail to deploy threats of equally costly retaliation? The first part of the answer is simple—U.S and foreign decisionmakers realize that to follow through with threats would be costly to the United States. A trade war with China might destroy China's economy but would also damage the U.S. economy, and a war of psyops with Russia might seriously damage the United States' relationship with many other nations. But these answers only explain part of the problem. Diplomatic bargaining is basic to international diplomacy. In most cases states are able to use a combination of threats and compromises based on their relative strength and diplomatic ability. In as far as the United States is far stronger in every way than its attackers, it is odd that it has been unable to defend itself.

Methods Attackers Use to Reduce the Risk of U.S. Retaliation

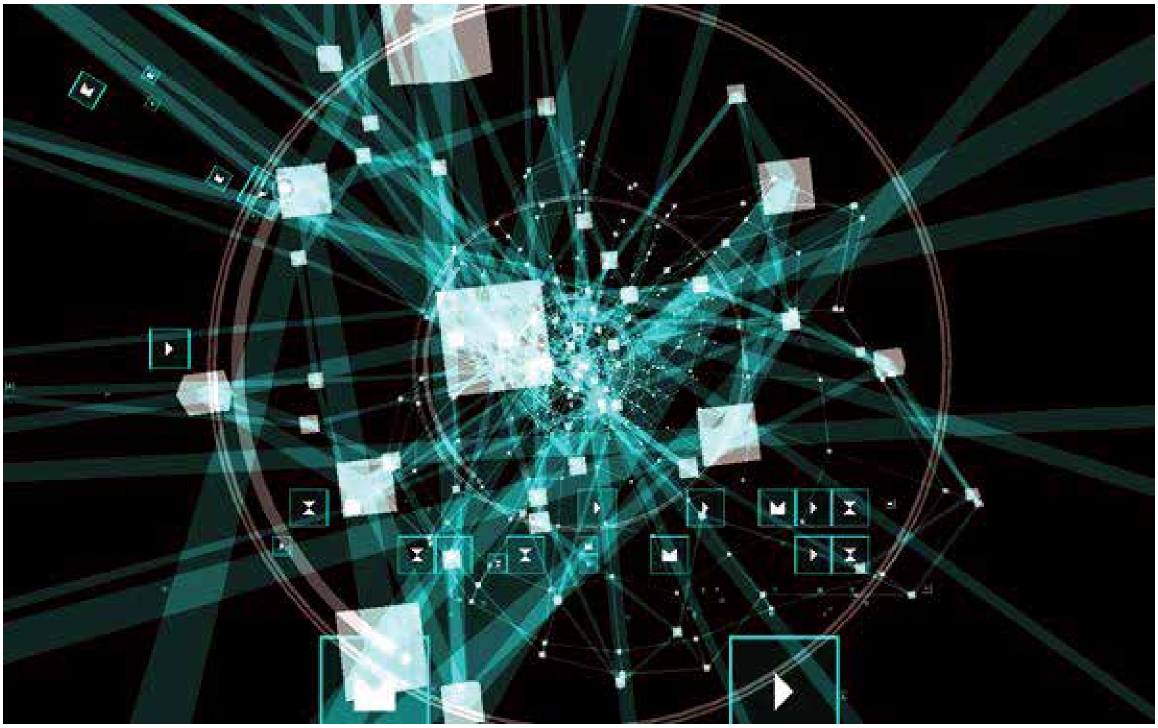
To understand America's reticence to make strong and credible deterrent threats, it is helpful to understand the tactics attackers use to undermine deterrence. A portion of these methods could apply to any type of gray space operation, while some are specific to cyber conflict.

Concealing Attribution

The first and most well-known method attackers use to dampen the threat of retaliation involves concealment of their identity. Because of the nature of cyberspace, attackers can often disguise the origin of their attacks or make the attacks appear to come from a third party. Even when a defender is able to trace the attack to a geographical location, it is often impossible to prove that the individuals at that location were acting on behalf of the government; states regularly conceal attacks behind facades of criminal organizations and patriotic militias. Even when the attackers can be linked to their governments, it is seldom possible to back such claims with the kind of evidence that would stand up in court or in the court of public opinion, and even when such evidence is available, providing it could reveal sensitive sources. Beyond this, attribution problems create incentives for third party nations to conduct false flag attacks designed to provoke conflicts between rivals. Knowing that this incentive exists, defenders have difficulty trusting even apparently clear evidence if acting on it would lead to conflict with the suspected attacker. In sum, even when defenders are relatively confident that they know the identity of an attacker, attribution problems create plausible deniability that can undermine the willingness to retaliate.

Concealing the Cost of the Attack

A second method regularly employed by attackers is to attempt to conceal the value of the attack. Hackers typically attempt to conceal the attack in its entirety. If an attack is discovered by the victim, hackers attempt to conceal the magnitude of the attack. Beyond this, however, the value of espionage, sabotage, and psychological operations is difficult to assess. When IP is stolen, it is not stolen in the traditional sense; rather, it is copied by the thief. It is difficult to assess the harm posed by IP theft, particularly when the evidence mainly resides in the territory of the pirating government. Not only do pirate states not cooperate with investigators, they often build elaborate domestic



The Defense Advanced Research Projects Agency's Plan X program is a foundational cyberwarfare program whose engineers are developing platforms DOD will use to plan for, conduct and assess cyberwarfare in a manner similar to that of kinetic warfare. (DARPA)

institutions specifically designed to disguise their actions. China, for example, has created a massive system of institutions and laws to launder stolen IP and "reinvent" it at home. Such techniques make it difficult to know when a cyberattack has occurred, to ascertain the magnitude and duration, and to assess the economic, security, or political costs—thereby complicating a defender's calculations when attempting to formulate deterrent threats.

Avoiding Symbolic Triggers

Cyberattackers regularly strike in ways that circumvent key psychological, cultural, and legal triggers. In democracies, acting on deterrent threats often requires public support. While national security professionals may be able to respond rationally to calculations, energizing the public often requires appealing to symbols. For instance, when Japan attacked U.S. battleships at Pearl Harbor in 1941, or when al-Qaeda attacked the World Trade Center and Pentagon in 2001, those actions triggered psychological reactions in the American public that had little to do with the economic and military effects on national security. In such cases, the public responds at least as much to fire, smoke, and casualties as to calculations about national interests. If Japan or al-Qaeda had attacked using computer viruses, U.S policymakers might not have gained enough public support to take the country into costly wars. Such dynamics incentivize attackers to stay clear of actions that are likely to trigger emotional responses. This tactic undermines the credibility of potential deterrent threats by requiring defending policymakers to make their case without the ability to appeal to the range of symbolic actions usually required to mobilize the public.

Using Asymmetrical Attacks

In deterrence bargaining, one of the central methods states use to signal intent and contain escalation involves asymmetric retaliation. The United States maintains a variety of instruments that provide it with escalation dominance in most arenas of competition, and Washington typically responds to hostile diplomatic action with diplomatic tools, economic action with economic tools, and military action with military tools. Understanding this dynamic, cyberattackers often attempt to attack the United States asymmetrically, in venues in which it cannot easily respond in kind. For example, China steals IP from the United States knowing that it has virtually no IP that the United States can steal in retaliation; it does not, however, attempt to undermine the legitimacy of the U.S. Government because it understands that the United States would most likely have symmetrical escalation dominance in such a contest. While the United States could threaten to retaliate against cyberattacks asymmetrically through economic sanctions or military threats, there is a significant chance that such actions would appear escalatory, disproportionate, or otherwise inappropriate to the American public or the international community. Consequently, as James Clapper alluded to in his testimony, such attacks complicate deterrence.

Employing Strategic Use of Time and Decision Cycles

In the United States, political leaders face regular elections and generally have short strategic horizons. This dynamic makes the United States particularly vulnerable to salami-slicing tactics. The idea is that an adversary can make as many small attacks as it likes, so long as the total value of the attacks remains beneath a certain threshold during a U.S. policymaker's decision cycle. A U.S. President may be aware that a decade-long campaign by Russia to infiltrate critical infrastructure would have consequences sufficiently dire to justify retaliation; but during any two year period, the results are not serious enough to justify a serious response. So long as elected officials think in terms of election cycles and attackers restrict the damage they do within these cycles they will be free to generate substantial long term results while minimizing the chances of retaliation.

Infiltrating and Manipulating

The United States is an open society, which means even its adversaries are allowed to attempt to influence or compromise the integrity of U.S. policymaking institutions. Russia and China spend large sums to hire highly respected former government officials with a track record of China or Russia bashing to lobby on their behalf; neither country has had trouble finding such officials.[7] China routinely sends hundreds of thousands of students abroad to increase its influence and access, while Russia regularly bribes and blackmails.[8]

Appealing to Reputation

When policymakers calculate how they will respond to an attack, they are often as concerned with their state's reputation as with the cost of the attack. A state that has a reputation for not retaliating against small attacks may come to be seen as an easy target for third parties. Thus, leaders might be willing to pay costs and take risks to avoid small losses that are disproportional to the apparent stake in a dispute. To the extent that cyberattacks are secret, however, this effect is dampened. If a defender loses something from a cyberattack and no one beyond the attacker and defender is aware, the defender may have a smaller incentive to worry about how an unanswered attack will affect its reputation.

Gray Space Deterrence

These tactics help to explain why the United States is regularly self-deterred from even attempting to deter cyberattacks. Its attackers have strong incentives to conduct attacks. This means the United States would have to threaten considerable harm to have much chance of deterring the attacks. Acting on such threats would be costly. Every action the attacker takes to reduce America's confidence lowers its willingness to make or act on costly threats.

To take a fanciful example, if a U.S. decisionmaker assessed that an adversary was conducting an attack on critical infrastructure from which it would eventually gain one billion dollars' worth of security, she might be willing to threaten the suspected attacker with sanctions that would cost the United States one billion dollars to execute. However, if she was only 80 percent confident that she had identified the actual attacker, she might only be willing to threaten sanctions that would cost the United States $800 million to execute. If, beyond this, she was only 80 percent confident that the attacks were truly having the assessed effect, she might only be willing to threaten sanctions costing $600 million. Further, if she was only 80 percent certain the public would see the threat as serious (given the lack of fire, smoke, or loss of life) her cost tolerance might drop to $400 million. If she feared that an asymmetric response, such as economic sanctions, would be costly to the United States' reputation, she might only be willing to bear $200 million in costs. If she believed that only part of the entire billion dollar price tag for the attack would accrue during her time in office, it might be preferable to wait and allow her successor to take the political risk of making the threat. Even if she were willing to take action, her belief in the efficacy of lobbyists acting on behalf of the attacker would further erode her confidence and willingness to place her reputation and political capital behind the policy. If she persisted despite these obstacles and the attacker did not assess that the cost of the sanctions would be higher than the one billion dollars in benefits it was gaining from the attacks, there is a good chance that it would not be deterred.

Real world cases are not as clear cut but this example helps to illustrate the calculations attackers and defenders must make in cyber conflict. If attackers attempted to use their cyber weapons without using such psychological tactics, it would not be particularly hard to deter them. Moreover, the success of these tactics is not entirely dependent on attribution problems or fear of counter-retaliation. Even in cases where the United States has identified attackers and done a good job of assessing the harm caused by their attacks, other dynamics have reduced its confidence to such an extent that decisionmakers have almost uniformly chosen not to act.

Conclusion

Most work on cyber deterrence concludes by advocating better defenses—this is excellent advice, but has so far failed to do much to reduce losses. A bolder approach would be to address each of the psychological tactics attackers employ. What is needed are improved ways to attribute attacks; study the actual cost of attacks; raise public understanding of those costs that do not result in obvious kinetic destruction; develop deterrence policies that operate across election cycles; and expose adversary attempts to illegally (and legally) influence U.S. domestic institutions. Such approaches would mark a departure from current policy but have the potential to undermine adversaries' psychological tactics and improve America's ability to deter cyberattacks. PRISM

Notes

[1] See for instance: Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016, available at < https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>; Michael Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," United States Army War College Press, December 2, 2015, available at < https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303>; Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," *Heritage Foundation*, 2016; Joseph Votel, et al, "Unconventional War in the Gray Zone," *Joint Forces Quarterly*, 1st Qtr, 2016.

[2] Mark Pmerleau, "Lack of Resilience Led to Lack of Cyber Strategy, Says Former DNI," *The Fifth Domain*, May 12, 2017, available at < http://www.fifthdomain.com/2017/05/12/lack-of-resilience-led-to-lack-of-cyber-strategy-says-former-dni/>.

[3] Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, March 24, 2016, available at <http://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF>; Jose Pagliery, "The Inside Story of the Biggest Hack in History," *CNN Tech*, August 5, 2015, available at <http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html>; Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," TIME, March 24, 2016; Andy Greenber, "How an Entire National Became Russia's Test Lab," *Wired*, June 20, 2017, available at <https://www.wired.com/story/russian-hackers-attack-ukraine/>.

[4] Geoffrey Ingolsoll, "Defense Science Board Warns of Existential Cyber Attack," Business Insider. March 6, 2013.

[5] Department of Defense, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics Washington, D.C. 20301-3140, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013.

[6] Elizabeth Dickinson, "Internet Freedom: The Prepared text of U.S. of Secretary of State Hillary Rodham Clinton's Speech," delivered at the Newseum in Washington, D.C. *Foreign Policy*. January 21, 2010.

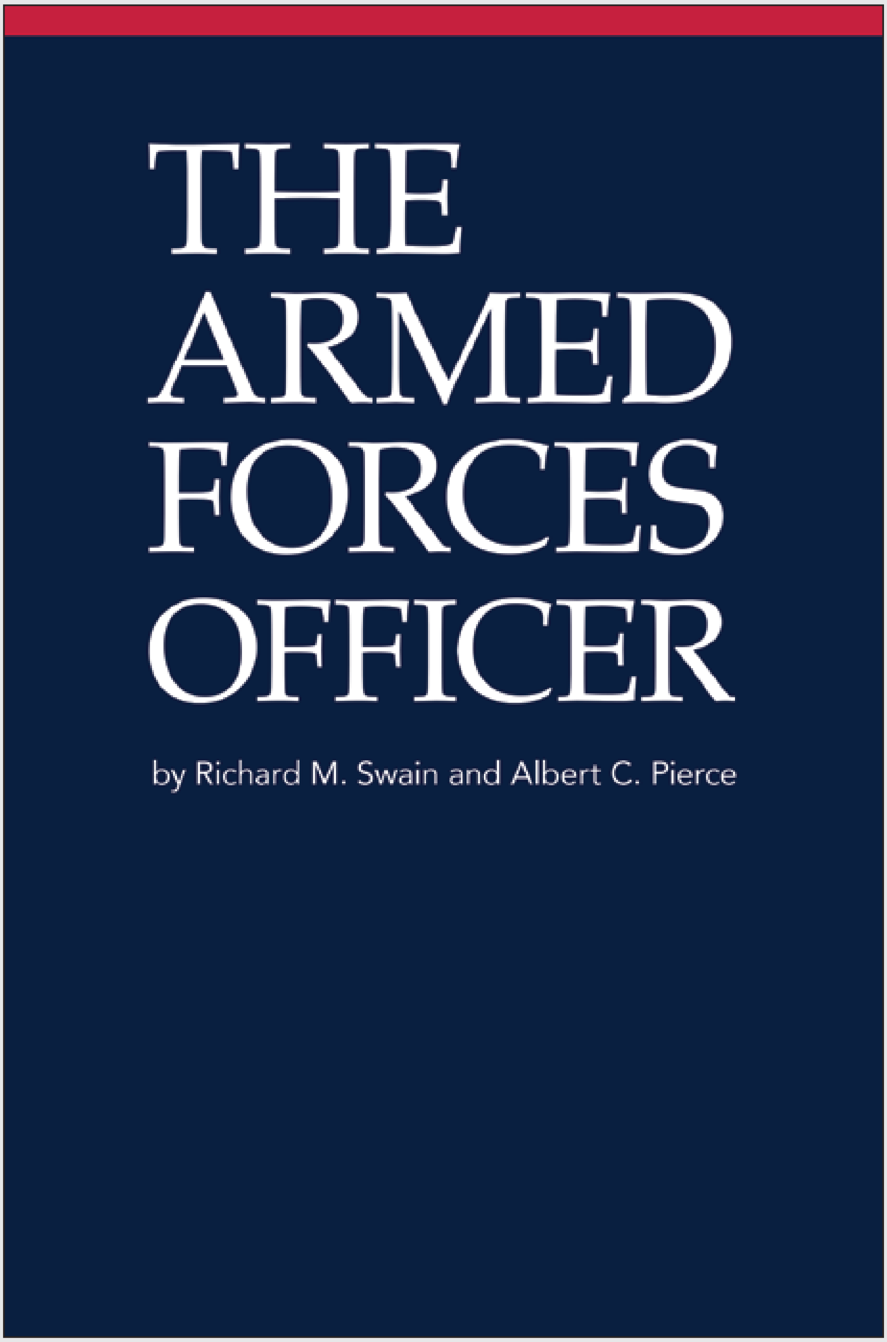
[7] For a good analysis of China's methods, see: Richard Daft, *Organization Theory and Design*, Cengage Learning, 2006,165. On Russia, see: Garrett M. Graff, "A Guide to Russia's High Tech Tool Box for Subverting US Democracy," *Wired*, August 13, 2017, available at <https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/?mbid=social_fb_onsiteshare>.

[8] John Garnaut, "Chinese Spies at Sydney University," The Sydney Morning Herald, April 21, 201, available at <http://www.smh.com.au/national/chinese-spies-at-sydney-university-20140420-36ywk.html#ixzz312tdddmi>.

Photos

Page 90: Idaho National Laboratory. From <https://www.flickr.com/photos/30369883@N03/7900490132/>. Licensed under Creative Commons Attribution 2.0 Generic License
<https://creativecommons.org/licences/by/2.0/deed.edn>. Photo unaltered.

Page 95: DARPA. Available at < https://www.defense.gov/News/Article/Article/758219/darpas-plan-x-gives-military-operators-a-place-to-wage-cyber-warfare/>.



THE ARMED FORCES OFFICER

by Richard M. Swain and Albert C. Pierce

Visit ndupress.ndu.edu to view the new edition, which includes a foreword by General Joseph F. Dunford, Jr., Chairman of the Joint Chiefs of Staff.

An airman prepares for a command cyber readiness inspection. (U.S. Air Force/Franklin R. Ramos)

Cyber Deterrence by Engagement and Surprise

By Jim Chen

The conventional deterrence strategies of denial and punishment do not factor in the unique characteristics of the man-made cyber domain. This domain needs a new and holistic deterrence strategy that involves prompt and direct cyber responses that are sudden, dynamic, stealthy, and random so that adversaries can be defeated mentally and virtually. This article offers such an approach that I refer to as "deterrence by engagement and surprise."

Deterrence

Released in January 2017, Department of Defense Joint Publication 3–0 defines deterrence as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[1] To make it effective, deterrence should depend on capability, credibility, and communication:

- capability helps to destroy what the adversary values most highly, thus making the cost of an attack exceed the benefit that an adversary could gain;
- credibility can be achieved via the demonstration of the willingness to use capability;
- communication requires capability, the willingness to use capability, and that credible consequences be made known to an adversary.

Simply put, deterrence is a coercive approach used for the purpose of avoiding a war or preventing the escalation of a war. It is used as a strategy to help achieve goals, and varied means can be adopted and diverse capabilities can be used to support such a strategy.

Our current deterrence strategies are heavily influenced by the nuclear and conventional deterrence models—deterrence by denial and deterrence by punishment. Strategist Herman Kahn held that defensive capabilities should be greatly enhanced to limit damage caused by an adversary, so that retaliation by the adversary can be countered, and a credible and real threat can be generated against the adversary during a conflict. In this sense, the capability to defend oneself for survival is a key element. This approach lays the foundation for deterrence by

Dr. Jim Q. Chen is a professor of Cybersecurity Studies in the College of Information and Cyberspace at National Defense University.

denial, which intends to scare an adversary away by denying his ability to inflict sufficient harm to justify the risk of retaliation.

Strategist Thomas Schelling, however, argued for the deterring effect of uncertainty in a stable balance of terror. He used uncertainties as the magic of threats since an adversary may fear irrationality or accident. As well explained by former Deputy Assistant Secretary of Defense Keith Payne, stable deterrence, which provides reliable, predictable, and mutual deterrence, "could be orchestrated to proceed from mutual prudence born of mutual vulnerability."[2] It is a strategy of having the other party be ultimately "persuaded to exercise self-control" because of the irreversible and disastrous consequences that may ensue without self-control. Payne retains, during the Cold War, the basic ingredients of this theory were the U.S. capability to threaten nuclear retaliation against the Soviet Union as well as the vulnerability of U.S. society to Soviet nuclear attack.[3] In this sense, uncertainties are involved in the outcome of this strategy as one does not directly control an adversary, who makes decisions on how to act and what to do. This approach lays the foundation for deterrence by punishment.

In the cyber domain, deterrence by punishment does not work well owing to the complexities of attribution and the challenges of stealth operations. To have a measure in place, deterrence by denial brings in responses from diplomatic, military, economic, political, legal, ethical, and other instruments of national power. If it is well prescribed, this approach can make an adversary feel the pressure and pain from multiple domains, thereby deterring further action in the cyber domain. However, this approach requires a well-orchestrated and near-perfect collaboration from all relevant domains—something that is difficult to achieve within a short period.[4]

The current DOD cyber strategy calls for a holistic approach, asserting that the deterrence of cyberattacks against U.S. interests will only be achieved through "the total of U.S. action, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S networks and systems."[5] If there is a gap in collaboration, however, the effectiveness of deterrence is immediately reduced.

A lack of a deterrence theory or a framework that accounts for the unique challenges in the cyber domain may account for the present ineffectiveness of cyber deterrence. The next question is how best to develop such a theory or framework to be effective in the cyber sphere?

Missing Components

An intensive study of deterrence indicates it is neither strictly an offensive nor defensive approach, despite a close relation to both. Offense and defense are focused on external factors while deterrence requires a near-simultaneous focus on both external and internal factors.

- The external factor reflects the unambiguous exhibition of power that serves as an enormous threat to the other side. This power projection is supported by unmatchable capabilities in number, volume, quantity, quality, size, and other relevant components.
- The internal factor reflects the intimidation truly felt by the other side. This overwhelming state is accompanied by the feeling of being exhausted, helpless, and defenseless. This can help to convince adversaries of the potential damage and failure that they are going to receive if they continue what they are doing. This psychological state could be reached through a number of factors, to include surprise. If surprise is so strong that it leads to a shock, intimidation may ensue.

Depending on the context, deterrence might have a closer relation to offense or defense. Offense, deterrence, and defense can be launched at nuclear force level, at physical force level, at cyber level, and at the diplomatic and economic level.[6] If offense, defense, and deterrence strategies are inserted into each level, a revised representation of levels can be generated:

- Nuclear force: Nuclear weapons can be used in an offensive operation and for nuclear deterrence. Missile defense systems such as the Terminal High Altitude Area Defense (THAAD) systems can be used for defense.
- Conventional physical force: In a small-scale conflict, automatic weapons can be used in an offensive operation or as physical deterrence. In this event, body armors such as bulletproof vests can be used for defense.
- Cyber: Cyber weapons such as denial-of-service tools can be used in offensive operations. However, they are not effective for cyber deterrence, as they are less violent than other means of deterrence such as nuclear weapons. Firewalls, intrusion detection systems, intrusion prevention systems, anti-malware tools are used for defense.
- Diplomatic and economic: Measures such as sanctions can be used in offense or for economic deterrence. Improving diplomatic and economic relations with third-party countries and adjusting internal markets are measures that can be used for defense.

Offense may restrictively be applied at the cyber level. However, there is no unique and effective deterrence at the cyber level.

Unique Characteristics of the Cyber Domain

Current cyber deterrence approaches are polarized, either focused on deterrence by punishment or on deterrence by denial. These approaches do not factor in the unique characteristics of the man-made cyber domain, which resembles a black box. Someone who uses a network connection and runs an operating system or perhaps an application, has no concept of how networks are connected, what codes are required for the operating systems, and what codes are executed for the application. Codes are run and processed at low levels while human machine interface occurs at a high level, supporting anonymity. When this anonymity is used in defense, it is privacy protection. When this is used in offense and in deterrence, it becomes stealth operations.

Given stealth, surprise can be generated at the user end; stealth maneuvers can be launched; and intelligence can be collected covertly, even with meta-data. Cyber feature sets, which include intelligence collection, stealth maneuvers, and surprise effect, can serve as force multipliers and eventually lead to military dominance if they are integrated appropriately into conventional military capabilities.[7] An examination of retaliation in the cyber domain reveals five unique features:

- Targeting is not an easy task, as attribution in cyberspace may require substantial time and effort. The delay in attribution affects deterrence by punishment more than deterrence by denial, as the former requires a target be accurately identified prior to any retaliatory response.
- Cyber weapons are not as severe as nuclear weapons or other physical weapons. There is no virtual massive destructive weapon like a nuclear weapon in the cyber domain currently, even though critical infrastructure might be targeted in an attack. In this sense, cyber retaliation is relatively limited in scale and capacity.
- Uncertainty is required for deterrence by punishment. It does not matter whether it is used in the physical world or in cyberspace.
- Retaliation is expected to be executed within a short period of time, especially in the cyber domain.

- Cyber weapons can generate unique effects that nuclear weapons or other physical weapons cannot generate. Likewise, they are good at generating surprise effects in the virtual environment, or in a combination of the virtual and physical environments.

Deterrence by Engagement and Surprise

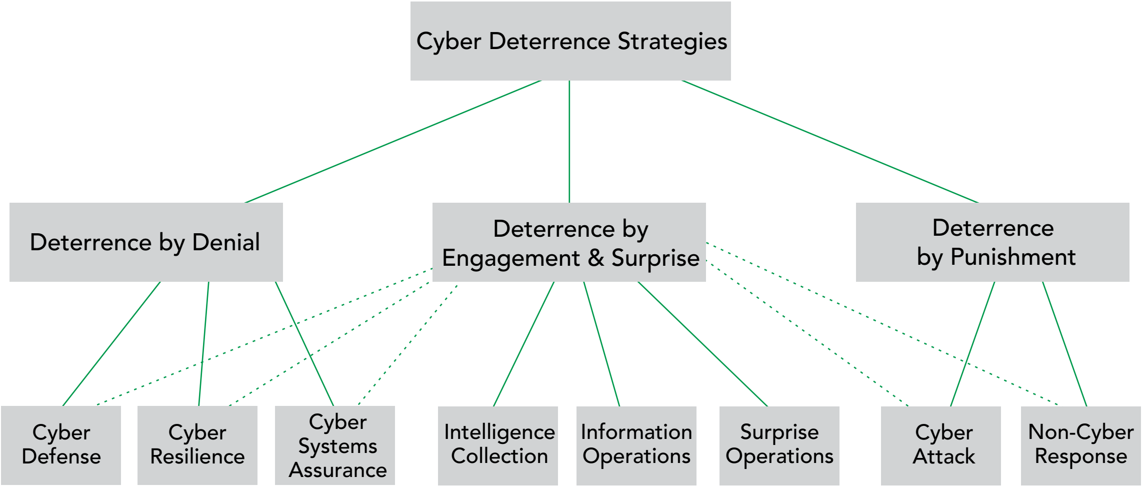
Deterrence by engagement and surprise offers the depth and flexibility to support sudden, dynamic, and random changes initiated by different contexts. Empowered by artificial intelligence (AI) and machine learning, this deterrence strategy is able to effectively and efficiently support intelligence collection, information operations, and surprise operations.

Intelligence Collection

Utilizing various intelligent sensors in varied parts of networks, collections engage the devices used by an attacker in revealing their true identity overtly and covertly via multiple channels and methods right after the devices that an attacker uses make abnormal requests. Such engagement, supported by machine learning, contributes to accurate attribution. It can eventually lead to precise and prompt targeting. Intelligent sensors can collect relevant information whenever necessary and feed it into machine learning algorithms. They take advantage of the fact that no hacker can control every single device along a transmission route in the internet environment. This makes it possible for such sensors to record the Medium Access Control (MAC) address and the Internet Protocol (IP) address of both the sender and the recipient in any leg of transmission. If the information of the previous leg is unknown, an engagement is initiated to chat with the device, such as a router, a switch, a proxy device, or a host device, to find out the relevant information. This capability can be built with the ability-to-learn algorithms powered by AI.

Artificial intelligence also makes it possible for a cyber weapon to mutate its appearance or even rewrite itself completely based on the context of when it is executed. In this sense, it is perpetually changing its behavior. In addition, different phases of maneuvers can be initiated from different parts of the world, thus confusing an adversary in finding out who sent out the responses. The dynamics built here help to create a stealth environment for cyber maneuvers.

FIGURE 1: Deterrence by Engagement and Surprise.



Information Operations

Advances in AI are able to drive change in information superiority. The capabilities for the collection and analysis of data as well as capabilities for the creation and manipulation of data can be dramatically improved. Disinformation and misinformation can appear persuasive. Meanwhile, "AI-enhanced forgery of audio and video media is rapidly improving in quality and decreasing in cost."[8] Likewise, AI can further improve electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), thus enhancing information-related capabilities (IRCs) "to gain advantages in the information environment" and "to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[9] All of these capabilities can be used to confuse and frighten adversaries.

Surprise Operations

Stealth maneuvers generate unexpected actions from various angles, aspects, directions, and locations, be it physical or virtual. The virtual munitions are loaded with varied payload. They range from audio warnings to light-weighted offensive operations. The virtual munitions are dynamically utilized based on contexts. A dynamic defense posture is thus created. This can successfully take an adversary by surprise psychologically, disabling his/her willingness to fight further or to continue the attack.[10]

AI systems can randomly select locations for launching surprise operations, which makes it difficult for an attacker to determine where the countermeasures are actually coming from. AI systems can also generate various responses, such as a surprise warning message, audio sound, web page, video clip, or anything that can warn or scare an attacker individually via different media. The purpose of surprise responses is to make an attacker realize the fact that he is under close surveillance and is responsible for what he is doing. This takes away the advantage of a covert cyberattack. Unless it is in an overt conflict, the attacker will withdraw from the attack in most cases unless he willing to receive the punishment. Meanwhile, evidence collection for digital forensics gets started. Determinant of the situation, a cyber offensive operation can also be launched as a retaliatory measure if it is legal and necessary. In addition, relevant diplomatic, legal, economic, and military measures can be taken.

This approach to deterrence can help foster a state of mind that decisively influences the decisionmaking calculus of the adversary who sees the intolerable consequence of aggressive action and who starts to fear such consequences.[11] Ultimately, this new approach is able to generate significant impact virtually, psychologically, morally, and physically.

Virtual

Virtual impact is achieved via intelligent responses from autonomous computer systems, supervised by humans if needed. Responses are usually at machine speed, avoiding any unnecessary delay. They are either defensive or offensive, or both, based on the specific situation, even though they are less severe. These responses are also precise as they are pointing exactly toward perpetrators with the help of collected intelligence. With respect to functionality, they can reject illegitimate requests, disable services, generate alerts, call in additional defensive forces, log abnormal events, back-track to find out the identity of the device that makes the initial request or even the individual who uses that device to make the initial request.

Psychological

This is achieved through surprise responses that range from a warning utilizing text, image, voice, or video messages on relevant devices including the initial device once discovered. These unexpected responses are manipulated by AI algorithms. Clearly displayed as an unambiguous exhibition of power via disparate capabilities, the responses are used to scare adversaries. When they suddenly realize that there are some unknown but powerful capabilities possessed by the opposing force, adversaries will reconsider the continuation of their attacks as they are not certain about the consequences of their attack actions. In this way, their cyber aggression can be dissuaded.

Moral

The moral impact is achieved via surprise responses that remind the user of the relevant devices of the moral and legal responsibilities they have in cyberspace.

Physical

The physical impact is achieved via intelligent systems under the close supervision of humans. It can cause disruption or destruction of a physical system.

Advantages of Deterrence by Engagement and Surprise

This new, holistic approach can successfully handle the challenge in a manner that deterrence by denial and deterrence by punishment cannot—it fills the deterrence gap. Engagement and surprise can lead to accurate attribution and precise targeting. It can also help to build a strategic buffer zone in the cyber domain and also help to eliminate the delay in responses as a whole. It applies not just to state actors but also nonstate actors and can help to avoid unnecessary escalation of conflict while providing prompt, dynamic, flexible, expandable, and effective retaliatory responses. This game changing capability offers at least nine advantages:

- It bridges the deterrence gap, thus enriching the theory and forming a holistic approach for which new deterrence mechanisms can be developed.
- Capability is exhibited in a unique way without delay and, during this process, credibility is enhanced through an effective display.
- The approach also addresses the unique characteristics of the cyber domain, so that responses can be generated at the cyber level thereby helping to avoid escalation.
- When contexts change, deterrence strategies can easily move upward or downward along the ladder of deterrence theory, which creates strategic depth.
- Prompt and direct responses are possible without conflict, be it virtual or physical. Warnings can carry several messages to include: close surveillance is on; further intrusion may escalate the situation; self-defense is initiated, and corresponding retaliatory responses will be generated.
- It applies Schelling's magic of threat—i.e. uncertainty in a new environment—thus adding new meaning to this old trick.
- With sudden, dynamic, stealthy, and random changes, deterrence by engagement and surprise is able to catch an adversary by surprise, thus defeating an adversary virtually, psychologically, morally, and physically.
- This new approach can also be applied to the physical world.
- Furthermore, the approach supports accurate attribution and precise targeting, which can support evidence collection for digital forensic investigation.

Conclusion

The cyber domain needs a new and holistic deterrence strategy that involves prompt and direct cyber responses that are sudden, dynamic, stealthy, and random so that adversaries can be defeated mentally and virtually. Deterrence by engagement and surprise is such a deterrence strategy. It takes advantage of the unique characteristics of cyber conflicts and creates a strategic buffer zone that makes it possible to dynamically select countermeasures based on specific contexts in addition to its support for intelligence collection, information operations, and surprise operations. Empowered by AI and machine learning, this deterrence approach is capable of exercising deterrence with virtual, psychological, moral, and physical aspects in an integrated way, thus leveraging cyber power (i.e. information power) together with diplomatic, military, economic, political, and legal power when dealing with challenges in the cyber domain. PRISM

Notes

[1] Joint Publication 3-0, *Joint Operations*, (Washington DC: The Joint Staff, August 11, 2011).

[2] Keith Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century*, (National Institute Press, 2008).

[3] Ibid.

[4] Current cyber deterrence strategists generally align with deterrence by punishment, deterrence by denial, or both. For more information on these please see: Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, vol. 33, no. 1, (2012), 148–70; Patrick Morgan, *Deterrence Now*, (Cambridge, UK: Cambridge University Press, 2003); Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, vol. 33, no. 1, (2012), 148–70. Eric Sterner, "Deterrence in Cyberspace: Yes, No, Maybe," *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*, (Washington DC: George C. Marshall Institute, 2011), 27; Frank Cilluffo, Sharon Cardash, and George Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability Through Strength," *Military and Strategic Affairs*, vol. 4, no. 3, (2012), 3–23; Martin Libicki, *Cyberdeterrence and Cyberwar*, (RAND Corporation, Project Air Force, 2009), 97.

[5] U.S. Department of Defense, *The Department of Defense Cyber Strategy*, (Washington DC: U.S. Department of Defense, May 2015).

[6] The levels of severity are based on the levels of belligerence as outlined by Martin Libicki in *Cyberdeterrence and Cyberwar*, (RAND Corporation, Project Air Force, 2009), 97

[7] For more information on this please see: Jim Chen and Alan Dinerman, "On Cyber Dominance in Modern Warfare," *Proceedings of the 15th European Conference on Cyber Warfare and Security*, (Reading, UK: Academic Conferences & Publishing International (ACPI) Limited, 2016), 52–7.

[8] See Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2017), 2, available at <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>.

[9] Joint Publication 3–13, *Information Operations*, (Washington DC: The Joint Staff, November 20, 2014).

[10] This is reminiscent to what Scott Beidleman explores in his work on "Defining and Deterring Cyber War," (Carlisle Barracks, PA: U.S. Army War College, 2009).

[11] See: Martin Libicki, *Cyberdeterrence and Cyberwar*, (RAND Corporation, Project Air Force, 2009), 8.

This copy of The Art of War by Sun Tzu is part of a special collection at the University of California, Riverside, and was likely commissioned or transcribed by the Qianlong Emperor (1711–99).

A Three-Perspective Theory of Cyber Sovereignty

By Hao Yeli

The cybercrime and cyber terrorism raging today are the most visible symptoms of a more pervasive problem concerning cyber security. How to establish a fair and just governance regime in cyberspace and establish international rules spark a storm of controversy. The controversy reflects the competing interests and demands of three distinct cyberspace actors: the state, the citizen, and the international community. By focusing only on one's own interests, each actor ignores the interests of the other two, resulting in the current situation in which each sticks to its own argument and refuses to reconcile. The establishment of a new order in cyberspace requires a comprehensive review from the perspective of all three major actors. This article proposes a "three-perspectives" theory based on the three actors. It divides cyberspace into three levels; the base level, the application level, and the core level. Treating each level differently, it seeks to identify the largest common ground, and transcends the single perspective vulnerability of interpreting everything in terms of binary opposition. Three-perspective thinking makes it possible to deal with the binary opposition of exclusivity and transferability with respect to state sovereignty.

Three Disputes Over Cyber Sovereignty

Cybersecurity has emerged as a global challenge and is becoming a tier one security threat for sovereign states. Heated debate rages in international forums concerning the rules of cyberspace, and the systemic and revolutionary challenges to global governance in cyberspace. Cyber sovereignty has inevitably become the focus of great controversy. Although a certain degree of consensus was originally achieved by the Information Security Group of Governmental Experts (GGE) of the United Nations, deep differences and doubts continue to divide the international community, particularly with respect to three issues.

First, the contradiction between cyber sovereignty and the spirit of the internet; the exclusivity of classical state sovereignty runs contrary to the spirit of the internet, which rests on the concept of unrestricted interconnectivity. If the emphasis is placed on cyber sovereignty, this may cause each country to set up a separate cyberspace of its own, thus resulting in the fragmentation of the internet.

Major General Hao Yeli, Chinese People's Liberation Army (ret.), is a senior advisor at the China International Institute for Strategic Society and a senior advisor at the China Institute for Innovation and Development Strategy.

Second, the contradiction between cyber sovereignty and human rights. This reflects the tension between the internet principle of freedom of speech, and state intervention in the name of cyber sovereignty, which restricts the free flow of information. Such criticism mostly targets the establishment of internet firewalls in China.

The third is the contradiction between cyber sovereignty and involvement of multiple stakeholders in governance. It is argued that cyber sovereignty will provoke controversy on the pattern of internet governance; that is, sovereign government-led governance will challenge the existing pattern of multi-party governance.

The concept of cyber sovereignty plays an important role in establishing the international rules of cyberspace. This is the root of the problem tree and the source of other problems. To clarify and resolve the differences, and to achieve international consensus and cooperation on these issues, are the challenges for the international community in the cyber domain.

The key is to adapt the traditional sovereignty concept to the globalized world in the cyberspace era with a more scientific approach and understanding of the controversies, in order to achieve the greatest common denominator and greatest acceptance by the international community. I am indebted to my Chinese and foreign friends and colleagues who participated in various international dual track dialogues—e.g. Sino–United States, Sino–Russia, and Sino–Europe—who gave me inspiration and insights into diverse perspectives. Even the most complicated problems can be solved with the correct approach. That encouraged me to build an objective theoretical framework and dialectical approach to clarifying and resolving contradictions.

Three Perspective Theory

In-depth analysis of these three major contradictions reveals the interests and demands of three main cyberspace actors: the nation-state, the citizen, and the international community. Focusing only on its own interests, each actor routinely ignores those of the other two, which has led us to the current situation, a situation in which compromise and reconciliation are difficult to achieve.

The actors behind the contradiction of cyber sovereignty and the spirit of the internet are the state and the international community. Behind the contradiction of cyber sovereignty and human rights are the state and the citizen. The contradiction of cyber sovereignty and multi-stakeholder governance involves the state, the citizen, and the international community.

Zero-sum games based on binary opposition usually lead to deadlock or the less than satisfactory outcome where “one succeeds, while all others sacrifice.” Today’s doubts and questions in the international community are the result of unilateral logic, one-way thinking, and viewing problems from a single perspective. When seeing things from one point of view, while ignoring the other two, one may tend to draw intractable conclusions that are either absolute or radical. We must transcend the single point myth and binary opposition, recognize a higher, holographic dimension, and adopt three-perspective thinking. To better understand the concept of the three actors and three perspectives in cyberspace envision a dark space with three lamps: lighting a single lamp enables us to see a point; two lamps reveal a flat, two dimensional surface; whereas, three lamps enable us to see the three dimensional whole. With three-perspective thinking, we can envision a more realistic cyberspace, where the roles and demands of each actor, as well as their internal relations and mutual impacts, converge to form a unity of diverse and contradictory opposites.

Theoretical Framework of the Three-Perspective Construct

In mathematics we always set boundary conditions in order to solve a multiple-equation problems ($n>x>0$). The variable is neither infinite nor infinitesimal when solving the equation in a range. The significance of the three-perspective construct is that we can set three boundary conditions from the perspective of three actors, which is more inclusive. It forms a stable triangle and co-viewing area to make effective dialogue to seek common ground, thus making the problem convergent, and focused to avoid one dimensional thinking that may easily lead to a "fire and forget" attitude.

Traditional and substantial national sovereignty implies natural exclusivity. It emphasizes the supreme authority internally, and stresses the inviolable independence externally, of the sovereign state. Because of the openness and global nature of cyberspace, however, the voices of the other two actors must be heard. When speaking of national sovereignty in this context, it is necessary to expand the perspectives of the international community and the citizen.

The citizen (or netizen in this case) pursues personal freedom. Today, the total number of netizens has reached 3.2 billion globally; in China alone the figure reaches 710 million. While also citizens of states and of the international community, it is in the nature of netizenship to pursue individual net freedom. In this disorderly environment, however, the fact is that individual self-governance based on self-discipline will not work, and freedom sought will have no guarantor. To ensure the freedom of every netizen, it is necessary to impose order so that cyberspace is bound and governed by the law. The establishment and formation of order requires external forces, as well as the establishment of rules at national or governmental levels to administer cyberspace and protect the legitimate rights and interests of netizens. Technology itself does not provide order nor security, so it needs sovereignty to provide appropriate legal protection.

The state pursues national security and development. A state has to ensure its safety while seeking development, and likewise must manage cyberspace while making use of it. At this point, the relationship between state and citizen is actually not antagonistic, but interdependent. In his speech on April 19th, 2017, Peoples Republic of China President Xi Jinping put it well when he said, "Cyberspace is people-centered. We should make the internet better benefit the people. The people on the internet equal public opinions on the internet. Our leading cadres go where the masses are; they must learn to follow the mass line through cyberspace and respond positively to the concerns and doubts of netizens." In China, we used to say that the party branch is organized on a company basis, but now, the regime must be built on the internet. We must listen to the voice of the people online, understand public opinion, pool their wisdom, and guide democracy; all of these reflect the intentions of the ruling Party. In the same way, the freedom and vigor of the internet will bring prosperity and national development.

The international community seeks openness and inclusiveness in cyberspace. The internet represents the mainstream of technological development, and a profound development of civilization. The international community must seek openness and inclusiveness, because there exist in the world not only competitions between the major powers, but also a collision of Eastern and Western cultures. Moreover, due consideration must be given to balancing the benefits of globalization and the digital revolution between the developed and developing countries.

The exclusiveness of national sovereignty and the openness of the international community while seemingly in conflict, can be reconciled and balanced in reality. On the one hand, the state must assume responsibility for emancipating minds, changing ideas, and promoting an objective and balanced understanding of the relationship between security and development. Only in this way can the internet work for us, helping us to maximize benefits while avoiding harm. A state integrates into the international system by transferring some portion of its national sovereignty, while international connectivity and interoperability will deliver greater developmental opportunities, promote cultural exchanges, economic cooperation, and collaborative security efforts. The relationship between the state and the international community is one of interdependence, inclusive and transferable, which contributes to the unity of opposites.

On the other hand, from the perspective of the international community, internet technology offers the promise of global interconnectivity. But as long as states exist, it is impossible to ignore national boundaries and national sovereignty. We ought therefore to avoid the excessive pursuit of unregulated openness, in order not to cross a tipping point beyond which global cultural diversity is subordinated to a single dominant culture. Those states with great cyberspace capacity should take the initiative to bridge the digital gap and actively transfer and share cyberspace resources and management experience, restraining their impulse to use asymmetric means in pursuit of narrower and short-term, national interests.

We would all benefit from more conjunction points of interest based on one global network to help all the countries of the world achieve economic growth, cultural prosperity, and security, all consistent with the spiritual essence of the internet: "interconnection and shared governance." Recently in China, certain prescribed terms of the new national antiterrorism law that aroused intense international concern, such as local data storage and interface providing, were deleted from the original draft. This shows that China is seeking to find the correct balance between openness and security.

States need to open up to the international community as they seek national security and development; citizens are in need of procedural safeguards from states in their pursuit of freedom; and the international community must tolerate cultural and national diversity in its pursuit of openness in cyberspace. These multilateral relations, though seemingly opposite and conflicting, are interdependent in reality. Actors cannot always blindly pursue absolute maximization of their own individual interests; they must demonstrate a certain degree of mutual consideration. Only thus will they reach an optimal balance in the triangular co-viewing area described above, existing peacefully in the global village of cyberspace.

In conclusion, the relationship between national development and national security is both a dynamic equilibrium as well as what we in China refer to as a yin and yang duality. Freedom and order, openness and inclusiveness are in fact both static and dynamic balances. The competing demands of these three actors are not in absolute conflict, nor are they absolutely contradictory, though in different contexts they will show a certain degree of antagonism. In the end, what we must all seek is an overall balance within the broadest context, built upon inevitable concessions, a desire for harmony, and acceptance of the principle of the possible unity of opposites. Through the exchange of ideas and the evolution of perspectives, we can resolve contradictions in many cases.

Cyber Sovereignty in the Three-Perspective Model

Although traditional sovereignty is naturally exclusive, cyber sovereignty must accept or at least consider a reasonable transfer of control in the era of globalization. Each state should carefully determine and decide what elements of sovereignty it must retain and what can be transferred, and to what extent. Let us further examine and analyze the concept of transferring partial sovereignty on the basis of the three-perspective model.

It is an uncontroversial fact that the debate on cyber sovereignty has been over whether or not sovereignty in cyberspace should be an extension of traditional sovereignty. Cyberspace has already become the fifth domain of conflict after land, sea, air, and space. The United States and NATO have both defined cyberspace as a battle domain and have created cyber combat troops. Although there are different formulations of cyber sovereignty, countries still regulate their own cyberspace to protect against external interference and damage without exception at a practical level. This reflects the recognition of practical cyber sovereignty requirements. Differences are not over whether or not we practice cyber sovereignty, but over which sectors cyber sovereignty will cover; in colloquial terms, will sovereignty cover the area "above or below the neck?" States have different "pain spots" concerning cyber sovereignty, and the international community must respect and understand the different concerns of states.

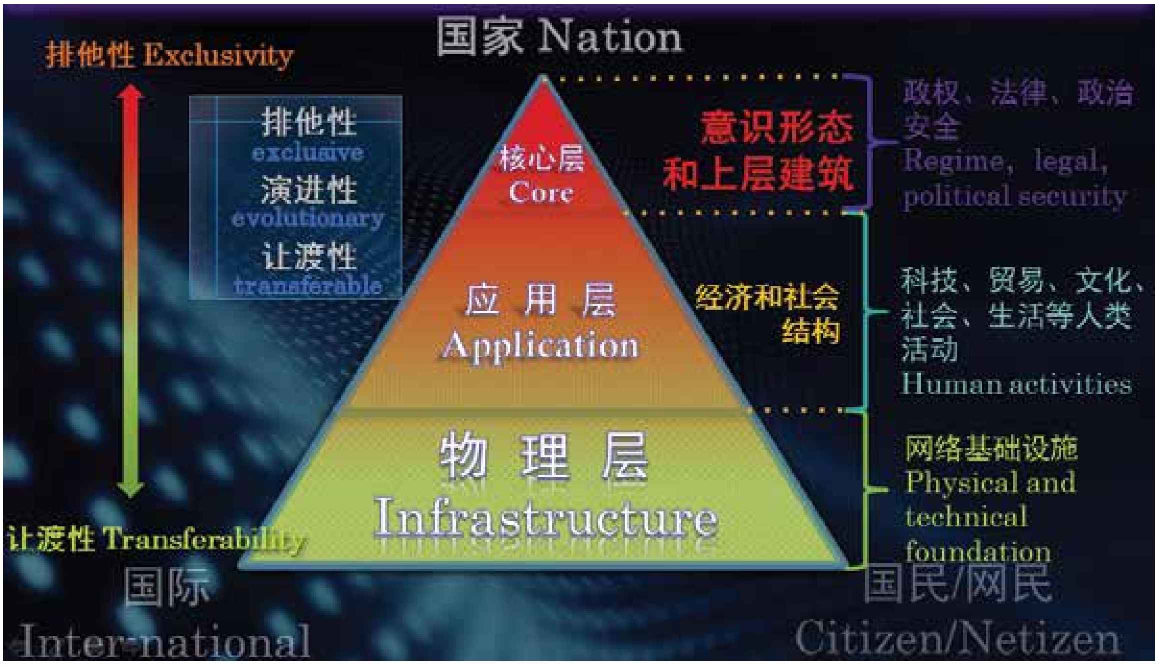
The key is to examine the divisibility of cyber sovereignty using a layered approach, and identify which elements of sovereignty must remain exclusive, and which are transferable.

In Figure 1 the lowest level, or the physical level, represents cyberspace infrastructure. The key at this level is the pursuit of standardization in global cyberspace and interconnectivity. At this level states should be willing to collectively transfer authority in the interest of standardization and interconnectivity. States with well-developed cyber capacity must take the initiative to extend standardization and connectivity to the less capable states; developed countries must export their achievements to developing countries to bridge the digital divide.

The middle level in the figure above represents the application level, and includes the many internet platforms and internet carriers in the real world that have integrated such different sectors as technology, culture, economy, trade, and other aspects of daily life. At this level, the degree of cyber sovereignty should be adapted to local conditions, with the aim to achieve dynamic equilibrium, multilateral, and multi-party joint administration, as well as balance between freedom and order.

The top or core level comprises regime, law, political security, and ideology, which is unchallengeable and includes the governing foundations and embodies the core interests of the country. Due to unique national

FIGURE 1: A Layered Approach to Cyber Sovereignty.



conditions, religious, and cultural backgrounds, legitimate differences do exist between states. Diversity is the norm of human existence which cannot be formatted according to any single culture. Differences and diversity should be tolerated. You may not agree with a country's social system and ideology, but you should understand its national conditions, respect its existence, and tolerate its differences.

It is clear that at the middle and bottom levels of the triangle, cyber sovereignty can be transferred to a certain degree, allowing a greater number of stakeholders to participate in governance, leading to a multi-stakeholder governance model. At the top level the emphasis remains on the leading role of the government. According to the consensus affirmed by the GGE "the right to make public policy on internet is part of a country's sovereign role, and each country naturally has judicial power over the information conveyed by the domestic information infrastructure." To respect countries' free choice of cyberspace developmental paths and cyberspace management models is a basic premise for both governmental responsibility and international cooperation.

A comprehensive understanding of these three levels further clarifies the differences between multilateral (meaning driven by state sovereignty) and multi-party governance modes. In fact, the two modes do not conflict; they have different applicability in different areas and levels of cyberspace. With respect to ideology, policy, law, institutional and governmental security issues, national governments will certainly give full play to their leading roles, and fully embrace the advantages of multilateral governance, while accepting multi-party governance at other levels.

Resolving the Contradictions

Earlier we noted the apparent contradiction between cyber sovereignty and the unrestricted spirit of the internet. There is no doubt that we live in "one world, one cyberspace." But exerting limited cyber sovereignty is consistent with the spirit of the internet; indeed cyber sovereignty is the necessary tool to help states participate equally in the global governance of the internet, contributing not only to interconnectivity, but also to shared responsibility.

We also noted the tension between cyber sovereignty and cyberspace freedom. As for setting up internet firewalls, China is forced to do so. Faced with the deteriorating security situation in cyberspace and the severe challenges posed by so-called color revolutions to developing countries that lack strong cyber capability, no country can remain indifferent to the real threats originating in cyberspace. We would not expect any country facing the everyday threat of terrorist attacks to dissolve its armed forces. Likewise, we oppose any cyberspace power taking advantage of its national capability to traverse the firewalls put in place by other countries. As the cyberspace security situation improves, and with the deepening of mutual trust, maturity of democracy, and the development of technology, China will continue to improve its accuracy in blocking harmful information and scale down the firewall. As we can see, the top level covers the smallest area, and excessive expansion of or preoccupation with the top level is not conducive to achieving consensus on cyber sovereignty among parties, which remains our ultimate objective.

With respect to the tension between multilateral and multi-party governance in cyberspace, advocating cyber sovereignty does not imply rejection of the multi-party or multi-stakeholder governance model. Governments are also among the multiple stakeholders; they should play appropriate roles in multi-party governance, but also respect and encourage other entities to participate in governance, including enterprises, communities, experts, and think tanks, taking advantage of their professional and technical contributions. Collectively we should prevent any stakeholder from excluding the participation of governments, or denying governments' appropriate role in key issues. At the core and application levels, the leading role of state governments must be ensured. When dealing with ideological, political, legal, institutional, and security issues the state role must be respected. For instance, the United States and Europe published the EU–United States Privacy Shield Agreement this year to eventually replace the abolished Safe Harbor Agreement, due to the Snowden leaks. The new agreement reflects in essence the implication of cyber sovereignty; meanwhile, it is the actual law practice in maintaining cyber sovereignty under the guidance of the government, which deserves our research and study. It is indisputable that government is the decisive pan-balance star in both international and domestic events. The government must act fast before it is too late. It is unavoidable that the government must assume responsibility and decide when to let go or to control.

The above analysis can be summarized as follows: in the cyberspace era, with the pervasive emergence of globalization, cyber sovereignty is divisible. The core level is inviolably exclusive, while the physical and the application levels are characterized by open and shared transferability. While challenging the core interests of sovereign states by abusing internet connectivity should be prohibited, shaking the foundation of the internet by imposing traditional sovereign exclusivity should also be prohibited. The proportion of sovereign transferability to exclusivity is flexible and ever changing, up to whether or not cyber sovereignty will be respected in the international rules.

Conclusion

Based on the principles of modern international jurisprudence, cyber sovereignty should reflect national rights and responsibilities. No state or government that is responsible and conscientious will ignore the development and security of this new domain. Nor should it reject or obstruct any other countries' reasonable demands concerning sovereignty and global co-governance. Respect for cyber sovereignty is a prerequisite for international cooperation in this domain, and the basis for the construction of a beneficial cyberspace order.

Against the background of globalization and the internet era, the emerging cyber sovereignty concept calls for breaking through the limitations of physical space and avoiding misunderstandings based on perceptions of binary opposition. Reinforcing a cyberspace community with a common destiny, it reconciles the tension between exclusivity and transferability, leading to a comprehensive perspective. China insists on its cyber sovereignty, meanwhile, it transfers segments of its cyber sovereignty reasonably. China rightly attaches importance to its national security, meanwhile, it promotes international cooperation and open development.

China has never been opposed to multi-party governance when appropriate, but rejects the denial of government's proper role and responsibilities with respect to major issues. The multilateral and multiparty models are complementary rather than exclusive. Governments and multi-stakeholders can play different leading roles at the different levels of cyberspace.

In the internet era, the law of the jungle should give way to solidarity and shared responsibilities. Restricted connections should give way to openness and sharing. Intolerance should be replaced by understanding. And unilateral values should yield to respect for differences while recognizing the importance of diversity. PRISM

Photos

Page 108: Wikimedia/O01326. Licensed under Creative Commons Attribution-Share Alike 4.0 International <https://creativecommons.org/licenses/by-sa/4.0/>. Photo unaltered.

An Interview with Marina Kaljurand, former Minister of Foreign Affairs of Estonia

You were the Estonian Ambassador to Russia during the 2007 cyberattacks against your country. Please describe those attacks—the effects of the attacks, and what Estonia learned from that experience.

Kaljurand: Those were the first explicitly political cyberattacks against an independent, sovereign state in history. If put into today's context, the attacks were not very sophisticated—even primitive. But back then, they were very disturbing. By that time, Estonia already had widely established internet and e-services, and an e-lifestyle; when those services were interrupted—mainly in the banking sector—it was highly disruptive. As to the effects of the attacks? They did not kill anybody, they were not destructive. They were highly disruptive to our lives though.

We have learned several lessons: First, you have to have your house in order, which means that you need an appropriate legal framework. You have to have strategies and action plans in place that clearly describe who is responsible for what. What are the obligations? What are the timeframes?

Second, we learned that efficient cybersecurity depends on an all-nation approach. Governments must of course have a central role in data security, but there must be an all-nation approach based on cooperation with other stakeholders, including the private sector, which plays a big role in cybersecurity and in providing internet services to the people. In Estonia, we were lucky to have assistance from the private sector from the very beginning of the attacks. Information and technology (IT) experts from the private sector volunteered to assist and support the government. A year later, a volunteer Cyber Defense League was created within the private sector, which symbolized the public–private partnership in real life, in practical terms. Today the League continues to work in very close partnership with the Government. Its members have security clearances and cooperate on a regular basis.

This interview was conducted by Mr. Michael Miklaucic in September 2017.

Partnership with industry is crucial, as is cooperation with academia. Although at the United Nations we have agreed that international law governs cyberspace—whether discussing countermeasures, sovereignty, or jurisdiction—the issues are very complicated; more complicated than most realize. So here, the expertise of genuine legal scholars from academia is important. Also necessary is cooperation with technical, and IT experts. That is the all-nation approach as we call it; where government has a leading role, but cooperates closely with other stakeholders.

The third lesson we learned is that cyberspace does not have borders. That means international cooperation is important. That is one of the reasons why we [Estonia] have been so vocal in international organizations, and have been very strong supporters of close, international cooperation; starting with international law, confidence building measures, capacity building measures, and all other efforts.

Given the inherent problem of attribution in cyberattacks, how can countries retaliate? And what are the principles that should govern retaliation against cyberattacks?

Kaljurand: The same principles that govern us in our offline life should govern us in the online dimension. We have the principles of international law—we have the UN Charter, Article 51 of which establishes for all countries the inherent right of self-defense—these principles are in place. In the case of cyberattacks, we should be guided by the same principles.

How does that work in practice? We are just now taking the first steps. Lawyers are interpreting and countries are starting to apply international law to the cyber domain. One of the measures of retaliation we used in 2007 was to put those we ascertained participated in the attacks onto the Schengen Black List.[1] I doubt at that time we really understood how powerful a tool that was. But, it worked. It was noticed. That was our reaction then. Other states have taken additional countermeasures. State practice in this regard is still developing and it will take time before we can say that we have effective and appropriate rules for countermeasures in the cyber sphere. The bottom line is that we have a basis in international law, and the same rules and principles that govern us in real life also apply to cyber.

In terms of state strategy would you advise that resources be invested in minimizing risks, or should states accept the risks and invest in improving resilience?

Kaljurand: There is no single solution. The solution must consist of different elements. If we look at today's cyber incidents, the majority are the results of human mistakes. Awareness-raising, education, and cyber hygiene have important roles, but we need additional measures for effective cybersecurity. For example, several weeks ago international experts discovered theoretical vulnerabilities in the chips of Estonian personal identification (ID) cards. Although the vulnerabilities were theoretical, we are undertaking corrective measures to avoid, or at least minimize the risks. You have to make it as costly and complicated as possible for those who want to attack your systems. Our experts estimate that it might take tens of years and 60 billion Euros to successfully hack Estonian ID cards—that is a high price. Not everyone is ready or able to do that; not everyone is willing to pay that price. This is a form of resilience—a way of making your systems secure. Those who want to attack systems will go for the ones that are more easily accessible or cheaper so that they do not have to expend so much in terms of human and financial resources.

I would also like to underline once again the importance of international cooperation and a common global understanding of what is allowed in cyberspace and what is not. It is important to agree among states, on the rules and norms of responsible state behavior. For example, reaching a common understanding that it is not acceptable to attack critical infrastructure, particularly financial systems or electoral systems, in peace time, and that appropriate responses will follow any such attacks.

Is that also a strategy for cyber deterrence?

Kaljurand: Professor Joseph Nye recently published an excellent article, "Deterrence and Dissuasion in Cyberspace."[2] In it he defines deterrence as a means of dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefiits. He lists four major deterrence mechanisms: threat of punishment, denial by defense, entanglement, and normtive taboos. In other words effective deterrence has multiple components; I agree we cannot rely on any single component.

I also believe in awareness raising and cyber hygiene. Some cybersecurity companies tell us we should accept that our systems/networks are already violated and compromised, and that we should dedicate financial and human resources to identifying violations and restoring the integrity and safety of the systems/networks. That might be one approach. But on the other hand it is important to teach our people, our employees, and our officials how to behave in the cyber sphere. Here, again, government has a central role cooperating with other entities, bodies, and institutions. Governments have to set the criteria, set the standards, and ensure that the standards are followed. This is another important step in reducing cyber risks.

We all know that it is impossible to eliminate all risks, either online or offline. The risks are different and are becoming more challenging with the development of information and communication technologies (ICTs). And it is the task of governments to minimize the risks, for both online and offline services.

In your view who or what are the most dangerous adversaries today in the cyber world?

Kaljurand: Cyber is a very difficult domain in this regard. It is a sphere which is relatively new, is developing very rapidly, and includes states as well as non-state actors. We have not yet seen cyberterrorism attacks, but we cannot assume we will not see them in the future. We have seen states supporting cyberattacks by private actors within their jurisdictions. We have seen illegal cyber activities by non-state actors. There are multiple players in the sphere, but what I think is important is that we take all of the necessary measures to ensure that cyberspace is ruled by law and by norms. We must ensure there is awareness of those rules, and awareness that if someone violates those rules, measures of retaliation will follow, in the same way as we do in real life.

It has been alleged that Russia, China, North Korea, and their proxies are the perpetrators of many of these cyberattacks. In your opinion, is their use of cyber tools, in any meaningful way, different from our own use of cyber tools?

Kaljurand: Speaking on behalf of my government, we [Estonia] have not hacked any elections, we have not interfered in the political systems of other countries. We are using legal means and, if we have problems with some policies of other countries, we use diplomatic means and do it in accordance with international law and international obligations, whether in the physical or the cyber sphere.

Estonia is a world leader in the development of e-government. Do you think that makes Estonia more or less vulnerable to cyber aggression?

Kaljurand: I think both. More vulnerable in the sense that we depend on internet services, which increases our cyber vulnerability. Some countries might not even notice when they are under cyberattack, but in our case, it was and will be acutely noticed. The 2007 experience showed that a country that has accepted or adopted an e-lifestyle is more e-vulnerable. So, on the one side, yes we are more vulnerable. At the same time, we are taking cybersecurity very seriously. According to the International Telecommunications Union, Estonia ranks 5th in the world and 1st in Europe in terms of cybersecurity. So we are doing pretty well, but there is room for improvement. Additionally, I would argue that we even have an obligation and duty to be leaders in cybersecurity—for the sake of our people and also because the international community is looking to us. In the end Estonia is the only country in the world to conduct online e-voting and the only country in the world that has opened some of its e-services (digital signature, e-banking, e-taxation) to foreigners through e-residency.

As I said earlier, a vulnerability was discovered in our identity cards. The chip manufacturer sells millions of chips to many other countries, but nobody else reported the vulnerabilities, because they are not using them [the chips] the same way we are using them. So, yes, it makes us more vulnerable but, at the same time, we have to be very good with cybersecurity.

I would like to return to an issue you raised earlier; international law and international cooperation. The United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security—the 2016–17 effort failed. Why do you think the GGE failed, and what steps have been taken since then to fill the gap?

Kaljurand: I have had the honor to serve on the 4th and 5th GGEs. It is absolutely regrettable that the present GGE failed—and I am using the word "failed," because our mandate was to reach a consensus report. We were mandated to look into several questions including emerging threats, norms and rules of responsible state behavior, applicability of international law, confidence building measures, and capacity building measures. We made progress in all of the fields, with the exception of international law. In 2013, the GGE agreed, and it was later adopted by the UN General Assembly and international community, that international law applies to the cyber realm. It was agreed in 2013 and reconfirmed in 2015 that the UN Charter in its entirety applies to cyber (or the use of ICTs). But in 2017, we could not agree to reiterate the assurances of Article 51 of the UN Charter guaranteeing the right of self-defense, countermeasures, and International Humanitarian Law (IHL). This is really, really regrettable.

What will happen next? I think it is too early to say. I think that we need a "cooling down" period. We need some time to look into what happened, why it happened, and where we stand today. Most probably we will have some parallel tracks. The ideological division between countries is so great that I am afraid that, in the UN framework, we will not be able to agree on the applicability of international law in the near future. I am not saying that the UN framework is not important, it is important—it is the only global framework we have, so we should maintain it. Maybe not in 2017, maybe in 2018 or even later. We should continue discussing cyber security in the context of peace and security with all countries that want to be part of the discussion. But we have to be very frank, and know that we will not have conclusive results in the near future, at least not on the applicability of international law. I see it as an awareness raising effort and an educational lesson. We must talk to countries who so far are not paying enough attention to cybersecurity; we have to engage more actively with them. I believe that concrete results on the applicability of international law and norms of responsible state behavior will first be reached within a group of like-minded states. And there are regional organizations. I am sure we can achieve concrete results within the EU and in NATO. The EU–NATO joint declaration and the recent EU cybersecurity package are proof of that. We should continue discussions among like-minded countries, while at the same time engaging with other states. It is our obligation to explain why our approach to cyber—promoting cybersecurity and cyber stability—is in the interests of all individual nations and the international community as a whole. It is our obligation to convince others that free, open, resilient, stable, accessible, and affordable use of ICTs can contribute to development and a better future for all people.

Can you tell us where the resistance was to the consensus in the most recent GGE?

Kaljurand: The resistance was to mentioning specifically Article 51 of the UN Charter, countermeasures in self-defense and the applicability of IHL.

China has recently taken a proactive role in the cyber domain, holding several conferences at which they articulated a view of cyber sovereignty that differs from the, if you will, Western view. Can you comment on their view of cyber sovereignty?

Kaljurand: The question of sovereignty was also raised by several of the GGE delegations, and yes, we do have different views on that. Our view, that is the Estonian view and my view, is that we cannot talk about absolute authority or sovereignty in international law. By acceding to international conventions—by accepting international obligations—we have already given up some part of our sovereignty. Acceding to the International Covenant on Political and Civil Rights, or any other international convention, imposes obligations on a state that effectively limit its sovereignty. Absolute sovereignty and international law are not compatible. Yet some countries continue to interpret state sovereignty as absolute sovereignty, unlimited by international law, subject only to national laws. That is the main contradiction.

What are the most threatening developments in the cyber domain today?

Kaljurand: The use of cyber by terrorists, which we have not seen yet, but we must anticipate. The Internet of Things brings to the internet and cyber arena many more actors, institutions, organizations, and individuals. Artificial intelligence. On one hand these developments have positive impacts on people, economies, and societies; and on the other hand they introduce additional cybersecurity challenges. We have to face the challenges, we have to get ahead of malicious intentions and actions in cyberspace. Cyber will not disappear. Cyber is here to stay, and smart countries will take maximum advantage of that. PRISM

Notes

[1] The Schengen area is an area comprising 26 European states that have officially abolished passport and all other types of border control at their mutual borders. Persons on the black list of any Schengen area country are denied entry to the entire Schengen area.

[2] Joseph Nye, "*Deterrence and Dissuasion in Cyberspace*," *International Security* 41, no. 3 (Winter 2016–17), 44–71, available at <http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266>.

Warnings: Finding Cassandras to Stop Catastrophes

By Richard Clarke and R.P. Eddy
Ecco, 2017
416 pp., $17.95
ISBN-13: 978-0-06248-802-2

Reviewed By Larry Garber

Every day we hear warnings—from parents concerned about the personal safety and good health of their children, to government officials worried about protecting the citizenry from external adversaries and the forces of nature. Distinguishing serious warnings of impending catastrophe from those that are frivolous may mean the difference between life and death, success and failure, freedom and oppression.

In *Warnings: Finding Cassandras To Stop Catastrophes,* Richard Clarke and R.P. Eddy focus on contemporary prophets—respected experts who issue warnings of dire consequences that will likely ensue if specific actions are not taken—and then evaluate the reasons their warnings are ignored or not acted upon with the requisite seriousness. The authors argue that we must pay particular heed to prospective Cassandras who have identified several non-strictly military threats and articulated the grave consequences that may result if their warnings are left untended.

The historic examples are of recent vintage—Iraq's invasion of Kuwait, Hurricane Katrina, Fukushima, rise of Islamic State of Iraq and the Levant—and will be familiar to most readers, even if the individuals who proved prescient in predicting these events are not. In general terms, the authors argue that government policymakers fail to heed the Cassandras' warnings because of their personal characteristics, the biases of those hearing their warnings, bureaucratic sclerosis, and prevailing political winds.

Based on the case studies presented, the authors devise a "Cassandra coefficient" as a guide to identify future disasters. Among the 24 factors that form the guide:

- initial occurrence syndrome—predicted event has never before happened;
- diffusion of responsibility among prospective decisionmakers;
- agenda inertia—too many items competing for attention;
- complexity mismatch—decisionmakers do not have the expertise to understand underlying data forming basis of threat;
- off-putting personality of predictor; and
- scientific reticence associated with predictor who, in rush to issue the warning, does not rely on complete data sets or followed precise protocols.

The authors emphasize that they are not proposing an algorithmic formula or trusting the wonders of big data for determining which threats to take seriously, but instead advocate relying on an analyst's subjective judgment of the factors comprising the Cassandra coefficient. The faith they place in the human Cassandra in this era of artificial intelligence and deep learning, at times, seems quaint.

The second half of *Warnings* examines seven prospective catastrophes—out-of-control pandemics; rising sea levels; nuclear winter; asteroid impacts; and technological advances associated with artificial intelligence; the Internet of Things; and genetic modification. The focus is directed toward scientists generally associated with prestigious academic institutions who issue the warnings. In some cases,

Mr. Larry Garber is a Senior Technical Adviser with Digital Mobilizations Incorporated.

the authors acknowledge that government bodies are debating appropriate responses. However, the authors warn against satisficing solutions, where the threat is the subject of further study or to responsive action not commensurate with the potential catastrophe.

Warnings can be read as an introduction to the implications of social psychology on policymaking when faced with uncertainty or as an overview of several specific challenges that contemporary policymakers must confront. However, the authors' evident intent—as evidenced by the bright yellow book cover and the *Warnings* title in large bold letters—is to dramatize the issues raised and to provoke debate among senior policymakers. Their broad goal is to influence those involved in national security matters.

In the final chapter, the authors call for the establishment of a new National Warning Office in the White House that would serve as the interagency focal point for identifying disasters on the horizon. They also advocate a series of responses under the general headings of surveillance, hedging, mitigating, and preventing. Finally, they emphasize the importance of applying a communications strategy to persuade reticent decisionmakers, cost conscious budget appropriators, an innocent public, and other nations of the need to act promptly and responsibly to counter the threats.

Surprisingly, given Clarke's and Eddy's respective experiences on the National Security Council, *Warnings* does not provide a guide for how to prioritize among the threats posed by adversary states—China, Iran, North Korea, and Russia—and the threats articulated by the new Cassandras. Currently, the traditional hierarchy of national security concerns preoccupies senior government officials in the executive branch. Their temporal bandwidths do not leave much room to prepare for the inevitable pandemics and sea level increases, much less the threats posed by asteroids or advances in technology that pose new dangers for humankind. These are perennial back-burner issues, which does not mean that no one in government is responsible for tracking them. Federal agencies, such as National Aeronautics and Space Administration, National Oceanic and Atmospheric Administration, Center for Disease Control and Prevention, and U.S. Agency for International Development, have experts who understand the serious threats described in the book, and they are feverishly seeking to devise appropriate responses even as they are starved for resources and their scientific knowledge belittled.

The policy question is how we determine, in our fast-changing and limited discretionary budget world, what is the appropriate amount of resources to invest in threat identification in general and as responses to particular threats once identified. In practice, such decisions are based on traditional political-economic considerations: who has the power, what incentives do they have to act, and are there countervailing factors that can impact their decision? For example, we are inclined to prioritize the eradication of extreme poverty or education for all, over preparing for an asteroid strike, even as research continues regarding remote, over-the-horizon threats.

Beyond the call for a new White House unit, *Warnings* does not consider whether the current architecture of the national security enterprise requires restructuring in view of the new threats. Many of the new threats reflect both stand-alone concerns for the United States and the potential for operational use by our adversaries. Hence, combating these threats requires a 21st century national security enterprise that consciously integrates the mission critical teams responsible for governance and resource allocations, operations and execution of programs, and the development and appropriate utilization of technological advances. These teams must provide the needed flexibility, particularly with respect to procurement and personnel, to ensure effective responses to existing and emerging threats.

All the prospective threats identified in *Warnings* represent challenges not just for the United States, but for the entire international community. Yet, the book gives short shrift to the role of global governance and the potential need for the development of new norms to cover such matters as the use of artificial intelligence, the internet, and gene editing in warfare, peacetime, and the gray periods in-between. The present era requires more inclusive processes, not just among nation states but including representatives of the private sector and civil society, and enhanced cooperation.

The authors do not consider whether their emphasis on the sentinel role of human Cassandras will remain practicable. Technological advances are increasing our reliance on machines to assess impending catastrophes and to develop appropriate responses. Indeed, it is not science fiction to anticipate increased reliance on Cassandra machines, which issue credible and timely warnings regarding the location of failing infrastructure, the occurrence of natural disasters, and imminence of health emergencies, and that contribute to saving millions of lives. And yet, while we expect technological advances, including super-intelligent machines, to improve personal well-being, human dignity, and freedom, humans must continue to play a leading role in ensuring that values remain an essential part of the equation. PRISM

International Conflict and *Cyberspace Superiority*: Theory and Practice

By William D. Bryant.
Routledge, 2016
239 pp., $54.95
ISBN-13: 978-1-13889-319-1

Reviewed By: Diana Gill

Cyberspace Superiority is a compelling mix of advanced technological know-how and easy-to-understand writing. Bryant, a Lieutenant Colonel who is a career fighter pilot and earned his Ph.D. in military strategy, first examines whether cyberspace is a "global common"—i.e. a shared resource like the oceans, atmosphere, space, and Antarctica. The answer may well determine the future nature of cyber hostilities but, with the issue as yet unsettled, Bryant posits a far more pressing question—is superiority in cyberspace "a useful construct for thinking about and planning for nation-state conflict in cyberspace?"

Loosely defined, superiority in cyberspace is a combatant's freedom to achieve "friendly objectives, while preventing the enemy from achieving his objectives." For the United States, this means our ability to operate freely in that environment without significant interference from enemy combatants during a time of war. Bryant likens it to superiority inherent to other domains of warfare—land, air, sea, and space—such as efforts by the U.S. Air Force to control air space, or the U.S. Navy to control the sea. He distinguishes cyberspace from the other domains by its extremely plastic nature. "Every computer, router, or device attached, or removed,

Dr. Diana C. Gill is an independent scholar and author of *How We are Changed by War: A Study of Letters and Diaries from Colonial Conflicts to Operation Iraqi Freedom.*

from cyberspace changes the cyberspace domain as a whole. We can think of an individual computer coming online as another grain of sand on the beach."

The virtual territory is only one aspect of cyberspace because of the "the many interdependent networks of information technology infrastructures that are not part of the Internet." Superiority in cyberspace is ever-shifting and disturbingly non-visual. Generals cannot ruminate over aerial photos of proposed battlefields. Satellites cannot pick up troop movements and positions. Sonars cannot pick up sounds lurking beneath the waves. Cyberspace is the ultimate stealth environment, but one which knits together the other domains. Bryant explains:

> *If an enemy disrupted command and control systems in the middle of a major land offensive, the loss of the cyberspace systems could result in the reduction of coordinated close air support over the battle and lead to the loss of the battle in the land domain. All the domains have connections but cyberspace is the most interconnected as combatants have embedded cyberspace in all the other domains through modern information systems.*

In this hypothetical situation of disrupted command and control systems, can cyber superiority be maintained by a combatant or is it analogous to a drive-by shooting—i.e. deadly but temporary? Bryant suggests that assessing an enemy's superiority is dependent on attribution; however, "the difficulty of attribution in cyberspace makes it challenging for defenders to understand where an attack is coming from and makes defensive responses more difficult." The shared nature of cyberspace and low cost of entry further complicate attribution since virtually anyone on the planet with technical know-how and a computer is a suspect.

Bryant explores weaknesses that allow some measure of control in cyberspace and includes in his discussion, analysis of attacks that focus on physical damage and those that affect information. The former can be caused by anything from dropping an actual bomb on a server farm to rewriting protocols to cause the equipment to self-injure. The trick with such attacks is in seeing them for what they are, rather than carelessly assuming them to be normal equipment malfunctions or software glitches. Once the defense becomes aware of what is happening they can quickly learn how to counteract the attack. As Bryant astutely notes, "Cyberspace weapons are akin to glass swords: they can be very sharp and lethal, but they tend to break on the first swing."

Also, unlike in the other military domains, superiority in cyberspace is not intended to be absolute—domination of every computer across the world is unattainable—and is best achieved at the local level. Precision attacks are the goal. Straining for too much superiority invites detection and wastes the valuable resource of time, which is better spent exploiting a small but pivotal foothold in an enemy's computer system. But even on the local level, the persistence of superiority in cyberspace is fleeting—seven out of the eight case studies showcased in *Cyberspace Superiority* lasted less than fourteen days. In closing, Bryant is quick to assert that while cyberspace superiority is highly desirable, it will not win a war by itself. It is merely a "significant advantage to a combatant who achieves it." PRISM

Cyberspace in Peace and War

By Martin C. Libicki
Naval Institute Press, 2016
496 pp., $54.98
ISBN-13: 978-1-68247-032-9

Reviewed By Julie Ryan

Martin Libicki has been a prolific writer in the field of information warfare since the mid-1990s. In this newer work, published by the Naval Institute Press, he aggregates his thinking during the past several decades into a single book. *Cyberspace in Peace and War* draws from work performed at RAND, both solely and with colleagues, and from lecture interactions with his students at various universities, to present a streamlined and consolidated overview of activities within and enabled by information technologies.

Before getting to the substance of this review, it is necessary to point out that this is a difficult book to read. *Cyberspace* is, in a word, dense. A naïve reader will likely have to do some additional research to truly understand the discussions and an informed reader will have to overlook stylistic annoyances so as to avoid getting lost in interpretative musings. For example, on page 73, Libicki uses the phrase, "hortatory injunctions." On one hand, the reader must pause to admire the sheer audacity of that phrasing. After, of course, looking up the definition of "hortatory"—tending or aiming to exhort—the phrase appears to be contradictory. An injunction is an order that either restrains desired behavior or compels undesired behavior. An exhortory injunction is a strange beast to contemplate—a command to act that requires additional exhortation? A command to stop action that requires additional exhortation?

Similarly, novice and expert readers alike may take exception to some of the more definitive assertions. For example, Libicki states that, "Controlling the effects of cyberattack entails controlling cyberwarriors." While it can be argued that cyberwarriors should be encouraged to limit the foreseeable effects of activities taken against cyber assets or against key terrain features of cyberspace, the fact is that it is impossible to control the unintended effects, particularly those that cascade, that result from cyberattacks. At the rate at which physical elements, such as light switches, refrigerators, or cars, are being integrated into cyberspace, the problem is going to get worse before it even has the chance to get better. Beyond that, some readers may also take issue with some of the language choices. For example, on page 145 Libicki says that "Originally all cyberattack operations came under the command and control of CYBERCOM." The purist will balk at that assertion, asking the question, "What about the cyberattacks that were performed prior to the creation of CYBERCOM?" After all, CYBERCOM was created in 2009—well after the ubiquity of networked communications systems created the reality of cyberspace. But these issues are distractions from the true value of the text, which lies in its breadth of coverage of cyber activities and thoughtful treatment of sensitive topics, such as equities.

Where *Cyberspace* shines is in its thoughtful treatment of philosophical questions. For example, Libicki invokes a variety of thought exercises to explore the nuances of operating in cyberspace. These include the so-called Las Vegas Rules—what happens in Vegas stays in Vegas—game theory, and effects versus means arguments. Exploring the

Dr. Julie Ryan is the author of Detecting and Combating Malicious Email and Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves. She joined the faculty of the College of Information and Cyberspace at National Defense University in August 2016.

arguments about what constitutes an attack, the functional equivalent of armed attacks, and rights of reprisal, he invokes customary law, norms, and influential publications such as the Tallinn Manual. Herein lies significant value. The reader need not agree with the conclusions to appreciate and benefit from the argument. Indeed, reasonable people do disagree on these issues, which are far from settled. Understanding the nuances of the arguments and the elements that underpin the perspective is a critical step to becoming an informed consumer.

A particularly useful part of *Cyberspace* is Libicki's treatment of deterrence. He explains concepts of deterrence, points of view from different players, and explores how deterrence might work out in different situations. The strategic focus of these discussions lays the groundwork for the reader to truly understand the interpretative reaction to actions taken in cyberspace, which then leads to the ability to make decisions about how different objectives might be achieved. His discussion is grounded in a discussion of law and the rule of law, which is far more important than a reader might imagine prior to indulging in this exploration.

Cyberspace is useful and can be a valuable resource. As noted by one reviewer, Robert Jervis, it is a "one-stop-shopping resource" covering the "range of issues, from the technical to the operational and political." The end notes are particularly useful for researchers, in that they point to contemporary sources as well as other publications that provide useful context and bibliographic grounding. At $55.00 for hard cover and $45.00 for a Kindle edition, *Cyberspace* is not inexpensive, but compared to other books, it is well worth the investment for the interested scholar. PRISM

POST2018

Pacific Operational Science & Technology Conference

March 5-9, 2018 • Sheraton Waikiki, Honolulu Hawai'i

On 5-9 March 2018, the U.S. Pacific Command (USPACOM) Science and Technology (S&T) Office, in conjunction with TechConnect, will host the **POST Conference at the Sheraton Waikiki Hotel in Honolulu, Hawaii, and the Hale Ikena Conference Center in Fort Shafter, Hawaii*.**

This year the conference will focus on "Transitioning Technology into Capability with our Indo-Asia-Pacific Warfighters and Partners". We are bringing together senior U.S. Department of Defense leaders from across the Services and Agencies, senior leaders from the international S&T community, industry executives and engineers, and university representatives and scientists to collaborate on how we can contribute to peace and stability in the Indo-Asia Pacific region through science and technology.

Science and Technology (S&T) is a critical enabler for improving operational effectiveness and efficiencies in a vast, diverse and complex area of responsibility. Join S&T leadership as we transition technology into capability with our Indo-Asia-Pacific warfighters and partners.

How To Participate:

- **Register** *(Advance Rate Through 19 January)*: https://events.techconnect.org/POST/
- **Exhibit/Sponsor:** https://events.techconnect.org/POST/exhibit_sponsor.html
- **Pacific S&T Poster Program** *(Abstracts Due 19 January)*: https://events.techconnect.org/POST/poster/

*Hale Ikena venue will host US/FVEY Sessions that require additional clearances. Visit POST site for details.

https://events.techconnect.org/POST/