VOLUME 2 ◆ NUMBER 1 2017

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

The Cyber Defense Review

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

CONTACT

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

SUBMISSIONS

The Cyber Defense Review welcomes submissions.
Please contact us at cyberdefensereview@usma.edu.

SUBSCRIBE

Digital: cyberdefensereview.org

The Cyber Defense Review (ISSN 2474-2120) is published quarterly by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.

∞ *Printed on Acid Free paper.*

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

BOOK REVIEW

The Cyber Defense Review

Introduction

VOLUME 2 ◆ NUMBER 1

The Cyber Defense Review: Rising Cyber Threat

Colonel Andrew O. Hall

VOLUME 2 • NUMBER 1 2017

THE CYBER DEFENSE REVIEW

Cyberspace in Multi-Domain Battle
Lieutenant General Paul M. Nakasone
Major Charlie Lewis

Clear Thinking About Protecting The Nation in the Cyber Domain	*General (Ret.) Keith B. Alexander* *Mr. Jamil N. Jaffer* *Ms. Jennifer S. Brunet*
Cybernomics – Changing the Economics of Cyber Defense	*Mr. Snehal Antani* *Mr. Ravi Iyer*
The Violence of Hacking: State Violence and Cyberspace	*Dr. Aaron F. Brantly*
Cyber (In)Security: Decision-Making Dynamics When Moving Out of Your Comfort Zone	*Mr. Andy Cohen*
Growing Role of Platforms in Cybersecurity	*Mr. Eric G. Troup*
INTRODUCTION *The Cyber Defense Review:* Rising Cyber Threat	*Colonel Andrew O. Hall*
BOOK REVIEW *Dark Territory: The Secret History of Cyber War* by Fred Kaplan	*Dr. David V. Gioe*

ARMY CYBER INSTITUTE • WEST POINT

INTRODUCTION

The year 2016 is likely to be remembered for many reasons, particularly as a notorious and profitable year for hackers of both nation and non-nation-state varieties. Over the last year, we have witnessed an Internet of Things (IOT) enabled Distributed Denial of Service (DDoS) attack that exceeded 1 terabyte per second, a resurgence of cyber information operations and a ransomware attack that impacted over 2,000 systems in the San Francisco Municipal Transportation Agency. Corporate offices, public agencies, Olympic athletes, political candidates, and tech CEOs were all directly targeted during a rather volatile year, all of which served to remind us of the personal nature of this fight. Aptly, Hackers were named as *Time* magazine's runner-up for Person of the Year.

As we have recently witnessed, the rising threat and growing complexity of the cyber environment can be overwhelming to even the most experienced and well-trained warfighter. This third edition of *The Cyber Defense Review* (CDR) seeks to inspire readers to pause and reflect upon the lessons of the last year. We offer viewpoints from senior leaders who remind us that despite the gains our cyber force and nation have made over the last several years, there is still room for growth. Starting with our Senior Military Perspective section, Lieutenant General Paul Nakasone (Commander, Army Cyber Command) and Major Charlie Lewis offer the Multi-Domain Battle concept and its applicability to cyber operations.

In our Professional Commentary segment, IronNet Cybersecurity leaders General (Ret.) Keith Alexander, Jamil Jaffer, and Jennifer Brunet offer clear thoughts on how best to defend our nation in an increasingly complex domain. To supplement these views, Andy Cohen discusses proposals for changing the way we think about our cyber

Colonel Andrew O. Hall is the Director of the Army Cyber Institute. He studied Computer Science at West Point, Applied Mathematics at the Naval Postgraduate School, and Operations Research at the Robert H. Smith School of Business at the University of Maryland. He has served on the Army Staff, Joint Staff, and deployed to the Multi-National Corps Headquarters in Baghdad, Iraq. He is a Cyber officer and was instrumental in creating the Army's newest branch.

environment and inspires a fresh understanding of how we go forward as a community. We also present an industry perspective from Eric Troup (CTO, Microsoft WW Communications and Media Industries) as he provides insights into the cybersecurity marketplace, and explains the growing role of platforms in cybersecurity.

Our Research section discusses the broader implications of the increasingly threatening cyber environment. In Dr. Brantly's article, he discusses the consequences of states behavior in cyberspace as they gravitate towards increasingly escalatory behavior. Dr. Chris Bronk and Gregory Anderson vividly layout the ISIL cyber menace and offer innovative policy recommendations to our national leadership. John Healy, Leland McInnes, and Colin Weir provide *CDR* readers with a brilliant article examining the power of analytics to meet the demands of Big Data. Major Micheal Kolton gives readers a provocative and penetrating look behind the 'Great Firewall' in his *China's Pursuit of Cyber Sovereignty.* This section closes with an article from Dr. Nicholas Sambaluk, Assistant Professor of Comparative Warfare Studies at Air University, who offers keen insights from West Point's defenses during the revolutionary war, and what lessons can be drawn for the digital age. Our winter edition concludes with the ACI's Dr. David Gioe's timely and engaging review of Fred Kaplan's *Dark Territory: The Secret History of Cyber War.*

Thank you for taking the time to read these keen insights from industry experts, scholars, and our senior military leaders. We hope you enjoy this edition, and that, more importantly, you are inspired by our author's cogent recommendations to deal with the challenges facing our cybersecurity environment.

The Cyber Defense Review

◇ SENIOR LEADER PERSPECTIVE ◇

Cyberspace in Multi-Domain Battle

Lieutenant General Paul M. Nakasone
Major Charlie Lewis

For months, a nation state has covertly infiltrated a neighboring state's critical networks while massing armored forces along its common border with a US ally. While the adversary prepares to launch a massive cyber-attack on its neighbor state, its tanks are readied to roll over the border. Nearby, a U.S. Division, engaged in an allied training exercise prepares to become the first line of defense against aggression. Unknown to the adversary, Allied and US forces have hardened their networks and at the first indication of aggression, have temporarily cut power to a nearby city to deceive the enemy. Simultaneously, a U.S. Navy warship fires an Electro Magnetic Pulse (EMP) missile at the adversary, disabling their electronic systems. Facing a numerically superior enemy, Allied forces, take advantage of the window of opportunity created by the EMP weapon to engage the crippled and confused enemy forces across multiple domains.

Today, United States superiority in any domain is no longer a guarantee. The continued low barriers to entry and use of relatively inexpensive cyberspace technologies may create advantages across any domain as well as the human dimension. Domination in any domain no longer makes for a successful military operation. Instead, leveraging multiple domains at specific points of opportunity creates the competitive advantage required to defeat adversaries on future battlefields. Recognizing this new paradigm, the Army and Marine Corps developed the Multi-Domain Battle Concept to deter and defeat enemies. [1]

Multi-domain battle is not a new concept. Throughout history, militaries have attempted to conquer their enemies by coordinating simultaneous attacks by land and sea, and later by air. The harnessing of the electromagnetic spectrum and the advent of modern communications technologies have allowed militaries with advanced warfighting capabilities to seize the advantage by engaging in multiple domain battle. *To win across a 21st-century multi-domain battlefield, the Army and Joint Force must first aggressively defend its networks, deliver cyberspace effects against its adversaries, and*

Lieutenant General Paul M. Nakasone assumed command of U.S. Army Cyber Command on Oct. 14, 2016. A native of White Bear Lake, Minnesota, the general is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

LTG Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. Prior to his appointment as Commander of U.S. Army Cyber Command, LTG Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command.

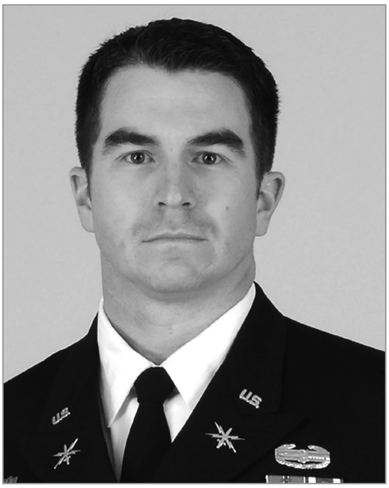
LTG Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and the Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

integrate cyber capabilities for the future fight across all domains.

During the early stages of World War II, Great Britain found itself exposed and threatened by imminent invasion from Nazi forces. The British military faced losing to a tactically superior and larger force, while the German Army marched across much of Europe virtually unchecked. German Wolfpack U-boat tactics closed shipping lanes, prevented critical resupply, impacted commerce and rendered the once great British Navy vulnerable. The British military faced invasion and defeat to the tactically superior and larger German force, a fact painfully played out, alongside French and Belgian allies during the Battle of Dunkirk and the fall of France.

Despite falling behind in three domains, the British development of radar at the end of the interwar period and utilizing integrated air and land defenses during the Battle of Britain proved pivotal. Using the electromagnetic spectrum, the British removed the element of surprise from the Luftwaffe. [2] Instead of waiting until spotters identified German aircraft by sight, the British employed an integrated air defense system that included radar, which provided a crucial over-the-horizon warning. British Army anti-aircraft batteries sat with rounds loaded while Royal Air Force fighters launched from airfields to engage the enemy in air-to-air combat. Radar allowed the British to maintain air superiority over the mainland and protect their naval defenses, thwarting Germany's invasion plans.

As evidenced by the British actions on land, sea, air, and the electromagnetic spectrums, combining efforts across multiple domains creates relative advantages that ultimately lead to victory. In preparing for a variety of conflicts, the Army and Marine Corps recognize that emphasizing one domain may lead to losses in battle. Instead, fighting across



A Cyber Operations Officer, Charlie Lewis currently serves as the Executive Officer of the U.S. Army's Cyber Training Battalion at Fort Gordon, Georgia. Commissioned in the Field Artillery, he first served as Fire Support Officer to Company Commander with 3rd Brigade, 101st Airborne Division. Following graduate school, he taught as an Assistant Professor in the Department of Social Sciences at USMA, serving as Department Executive Officer his last year. Most recently, he directed the Cyber Leader College at the U.S. Army Cyber School. His military education includes the Army's Ranger, Airborne, Air Assault, Pathfinder, and Combat Diver schools. Charlie is a 2004 graduate of the United States Military Academy and holds a Master's in Public Policy from Harvard University. He is an Assistant Editor for Army Cyber Institute's *The Cyber Defense Review* and a Term Member on the Council on Foreign Relations. He recently served as a Madison Policy Forum Cybersecurity Fellow.

multiple domains, including cyberspace, increases the effectiveness of US forces while adding complexity to the battlefield. Success in this new concept relies heavily on the integration of cyberspace operations, which this paper defines.

A NEW WAY OF THINKING

Chief of Staff of the Army, General Mark Milley offered, "... we are on the cusp of a fundamental change in the character of war." Changes in technology, geopolitics, and demographics are shifting how American forces fight wars.[3] Preparing now to allow the Army to meet simultaneous challenges across all domains is imperative if we hope to avoid first battle losses. The velocity of future conflict demands that we not wait for our adversaries to adopt new techniques and technologies.[4]

American technological overmatch has ceded territory to near-peer adversaries, regional threats, and non-state actors.[5] According to the Chairman of the Joint Chiefs of Staff, General Joseph Dunford, the proliferation and rapid development of technologies makes it easy for not only Russia and China to close the American advantage, but also for smaller actors to "frustrate U.S. interests".[6,7] Even as the Joint Force uses robotics as force multipliers, improved radio-frequency weapons, and continues exploitation of vulnerabilities in weapons systems, adversaries will keep pace and do the same.[8] Swarming formations of robots, micro-Unmanned Aerial Vehicles, and various other technologies will create confusion and overwhelm US decision-making in future battles.[9] Adversarial technological adoption can render US firepower impotent, no matter how powerful, before crossing the line of departure unless the military prepares for new technologies.

Advancing the proven success of combined arms in a joint environment, the Multi-Domain Battle Concept envisions future ground combat forces providing commanders options across multiple domains to deter and defeat adversaries while working with a variety of different partners. This concept will apply combined arms maneuver across all domains to create multiple dilemmas for the enemy.[10] Dominance across all domains all the time is not required. Instead, Commanders will maneuver within each domain at a given point in time to create windows of opportunity and temporary domination to gain the advantage.[11]

Multi-Domain operations rely on interdependent networks that also serve as the base for the cyberspace domain.[12] Presenting both opportunities and vulnerabilities, cyberspace serves as a significant option for strategic operations.[13] It is up to our cyber forces to prepare for victory across the information environment.

DEFENSE OF NETWORKS, DATA, AND WEAPON SYSTEMS

Well before any battlefield engagement on land or in air, Army Cyber forces enter combat against an enemy set to disrupt US network operations. Small elements of cyber defenders protect tactical networks, responding to breaches of integrated air defense systems. Soldiers continue to update systems, ensuring each weapon and tactical warfighter possesses the latest patches or logical armor. Back at Fort Gordon, Cyber Protection Teams defend broader swathes of networks remotely, hunting for advanced persistent threats, and maintaining the strategic picture to defend cyber key terrain to enable mission command.

> To win across a 21ST century multi-domain battlefield, the Army and Joint Force must first aggressively defend its networks.

Without the network, there is no Multi-Domain Battle. The sinew of maneuver across all domains is the network.[14] Army forces are not just reliant on the network for communication and operations; the network is also the weapon system upon which all cyber forces project power. Failure to defend the network exposes cyberspace's base of operations. Like its old coastal artillery mission, the Army must recognize that defending well in one domain requires defense across all others. Admiral Harry B. Harris, Jr., described the Army's role as "defending the sea from land."[15] Coastal artillery enhanced the ability of other domains to deny access to the enemy by protecting logistics hubs, seaports, and airbases.[16] Cyber forces protect the network through layered defenses while also securing air, sea, and land force communications. Complexity with serial defense in-depth hinders enemy operations while enabling friendly maneuver.

Cross-domain defense starts with each domain defending itself first. Because what was once a minor nuisance—cyber-attacks—can now inflict damage with significant military implications, effectively operating and defending the network must be the first priority of all operations.[17] Threats against our networks eclipse current potential gains achieved through offensive cyberspace operations. Moreover, as we look for greater capabilities within cyberspace, we become even more vulnerable to adversary intrusions and preemptive strikes.[18] The importance of effectively operating and defending our networks cannot be overstated.

The enemy seeks information and each user on the Department of Defense Information Network (DoDIN) provides an avenue of approach to their objective. Securing the DoDIN not only allows ground forces to communicate across domains, but it also allows offensive cyberspace operations to maneuver into enemy terrain. Unity of command across cyberspace, allowing for both the operation and defense of the network will better integrate defenses within cyberspace.

> The velocity of future conflict demands that we do not wait for our adversaries to adopt new techniques and technologies.

Fortifying the network affords commanders opportunities in other domains by enabling mission command. Various warfighting components from aviation to fires must communicate with land forces while maneuvering to access information on adversaries, the terrain, and the disposition of friendly forces. Gaining and maintaining a decisive advantage in conflict requires accurate and timely decisions based on information gathered.[19] The network allows for the sharing and consolidation of data across various organizations, commands, and even domains. Intelligence reporting, orders, targeting, and execution commands will not happen unless there are strong and secure lines of communication. The synchronization and integration necessary to win across a multi-domain battlespace cannot occur without the network.

DELIVERING EFFECTS AGAINST OUR ADVERSARIES

Army Cyber operators move through enemy networks. Enemy battle plans disappear while supply trains fumble through traffic jams created by incorrect orders and railroad signals. Adversarial forces receive confusing messages about their leaders abandoning them via social media while preparing their equipment. Enemy observation drones crash due to signal jamming from electronic warfare forces at the front lines.

One domain can create “temporary windows of advantage” for another.[20] Extending the battlefield over multiple domains provides commanders options to exploit vulnerabilities when they appear as opposed to engaging based on linear constructs.[21] Just as the British exploited the electromagnetic spectrum with radar to grow their engagement area during the Battle of Britain in 1940, cyberspace must do the same today.[22] Delivering effects against the enemy through the network and across the information environment empowers US commanders while increasing the complexity of the battlefield for the adversary who will not know where Army cyber forces lurk in their networks.

One of the goals of the Department of Defense's (DoD) Cyber Strategy is the "need to maintain viable cyber options" integrated into plans to achieve precise objectives.[23] To meet this goal, cyber forces project power through cyberspace in support of various levels of command. From development to employment, cyberspace effects must connect to commander's intent and objectives. Cyber forces must use their diverse problem-solving skills to anticipate requirements and create tools and capabilities to meet requirements. Unlike artillery shells or bombs, cyber tools are limited and may even be a one-time use system. While ground forces can call for multiple artillery rounds to destroy a power transformer, cyber forces may have one opportunity to deliver their capability to destroy the same piece of equipment. Commanders must synchronize their use during the right window to apply resources wisely within the cyberspace domain.

> The network is also the weapon system upon which all cyber forces project power.

Beyond networks, attacking through the electromagnetic spectrum provides another option. Electronic warfare successfully supported recent Russian land operations in Crimea and demonstrated how swarming of threats across multiple domains confuses an enemy.[24] Currently, electronic warfare capabilities reside at the tactical level, providing ground commanders responsive and flexible options to conduct an electronic attack, support, or protect. Using the equipment and talent located within their formation, commanders can incorporate fires through the electromagnetic spectrum to support their maneuver operations. By jamming enemy communications at a given point while also masking their own signatures, ground forces can move freely across the battlefield. No matter what method of operation within cyberspace, gaining a temporary advantage, in conjunction with combined arms maneuver, increases the adversaries' complexity. Cyber forces must deliver effects in creative ways to maintain this advantage.

INTEGRATED CAPABILITIES

US forces maneuver to regain border towns lost to enemy forces. US aircraft race overhead and artillery screams past their buildings, but the munitions only land on the vehicles camouflaged outside of the town. As an enemy detachment keys their microphone to report activity, a message comes across their computer telling them to surrender and providing the current grid of every soldier in that town. US troops maneuver closer, releasing a swarm of drones. Electronic warfare operators start spoofing the size of the small force, confusing enemy leaders who now think it is a battalion. Panicked, forty enemy combatants surrender their *defenses. A drone developed by an Austin startup flies to each enemy soldier, scans their irises, confirms accountability, and relays directions. An Electronic Warfare specialist jams any potential enemy communications as they surrender, not to a battalion, but instead to an expeditionary cyber team of five personnel.*

From defense to offense, capabilities must span cyberspace, electronic warfare, and information operations. Just as British leaders exploited a new technology, radar, to gain an advantage over the Nazis, joint force commanders must do the same today in support of Multi-Domain Battle. Developing new cyberspace capabilities starts with framing the problem and then innovating throughout the integration process. New DoD initiatives stress the research and development cycle but more is needed to meet the speed and agility required by the Army.[25] Over the past decade, adversaries created new products, spent more money, and even pilfered American research to counter traditional US strengths.[26] To regain the advantage, DoD has undertaken numerous initiatives to accelerate the acquisition process of cyberspace technologies, including Defense Innovation Board, the Strategic Capabilities Office, and the Defense Innovation Unit Experimental (DIUx).[27] Instead of years in development acquisition, the Army hopes to purchase capabilities and deploy them much faster in support of ground forces.

> Cyber forces must use their diverse problem solving skills to anticipate requirements and create tools to meet requirements.

Equally important, force structure and education shifts must occur to incorporate new technologies. Commanders must integrate the opportunities new capabilities provide as rapidly as acquired.[28] Preparing commands through professional military education's new emphasis on cyberspace increases Army leaders' understanding of cyber threats and cyberspace capabilities. Today, opportunities exist to enable commanders with cyber and electronic warfare capabilities against the Islamic State in Iraq and Syria along with fulfilling U.S. Army Europe's call for an urgent operational need to address current warfighting shortfalls.

The Army's Cyber Electromagnetic Activity (CEMA) Support to Corps and Below (CSCB) initiative today demonstrates how cyberspace operations can be integrated into a combined arms maneuver force to succeed at lower echelons.[29] Moreover, While Electronic Warfare (EW) personnel provide planning prowess, their minimal structure limits operations across the entire cyberspace domain. However, CSCB efforts integrating EW with Cyber, Information Operations, and Intelligence personnel, equipment, and capabilities provide commanders with offensive and defensive cyber capabilities to gain an advantage in a domain previously limited to them.[30] Moreover, CSCB shows forces how to adapt processes and use their organic Electronic Warfare cells.[31]

Even with force structure and weapons platforms, commanders must also visualize cyber terrain the same way they do land to understand the battlefield.[32] From maneuvering forces to de-confliction, visualization mitigates conflicts within the military and interagency, allowing for a faster response to adversarial actions.[33] Finally, visualization can lessen one of the main risks in cyberspace, crossing into another area of responsibility. Authorities constrain operations to limit risk because many cannot see the ultimate effect; adding a picture can show full movement on the battlefield and will speed up the approval process.

One of the goals of the DoD Cyber Strategy is the need to maintain viable cyber options integrated into plans to achieve precise objectives.

CONCLUSION

Confused, the enemy retreats well beyond the border. US forces overwhelmed their decision-making processes and information flow. Key communication devices crashed. A numerically inferior US and allied force somehow defeated a well-defended force connected to its logistics bases. Fighting over multiple domains created a complex battlefield the enemy could not control or defeat.

Multi-Domain Battle succeeds when each domain gains the advantage in support of others, requiring innovative approaches to integrating cyber operations, just as the British did with radar. A failure to layer operations across multiple domains creates gaps that adversaries will expose. Combining maneuver across domains creates many dilemmas for the enemy. The network today is the piece that best ties operations across all domains. With the network connecting all domains, success within cyberspace is imperative. From defending the network as a base to achieving effects against the enemy, the Army must prepare to fight in an environment that changes exponentially and will look much different tomorrow. Starting with the defense of the network, cyberspace protects “bases” upon which offensive forces can deliver effects through fiber and the spectrum. Integrated throughout the levels of command, the cyberspace domain’s integration in multi-domain conflict will be critical for future Joint Force commanders.

NOTES

1. David Perkins, "Multi-Domain Battle: Joint Combined Arms Concept for the 21ST Century" *Army Magazine.* Retrieved on November 22, 2016 from https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms-concept-21st-century.

2. Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States." *In Military Innovation in the Interwar Period,* edited by Williamson Murray and Allan R. Millett, Cambridge: Cambridge University Press, 1996, 265, 299.

3. General Mark A. Milley, "Changing Nature of War Won't Change Our Purpose,"*AUSA Greenbook 2016-2017,* October 2016, 15-16.

4. First battles comment based on *America's First Battles, 1776-1965,* edited by Charles Heller and William A. Stofft.

5. "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World," *Joint Chiefs of Staff,* Washington D.C., 14 July 2016, 15.

6. General Joseph Dunford, "Posture Statement of General Joseph Dunford Jr., USMC, 19TH Chairman of the Joint Chiefs of Staff Before the 114TH Congress Senate Armed Service Committee Budget Hearing," *United States Senate Armed Services Committee,* March 17, 2016.

7. "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World," *Joint Chiefs of Staff,* Washington D.C., 14 July 2016, 15.

8. "Joint Operating Environment 2035," 16-19.

9. Paul Scharre, "Unleash the Swarm: The Future of Warfare," *War on the Rocks,* retrieved from http://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/ on December 28, 2016.

10. Albert Palazzo and David P. Mclain, III, "Multi-Domain Battle: A New Concept for Land Forces." *War on the Rocks.* Retrieved from http://warontherocks.com/2016/09/multi-domain-battle-a-new-concept-for-land-forces/, accessed November 22, 2016.

11. Perkins.

12. "Joint Operating Environment 2035," 33.

13. "Joint Operating Environment 2035," 33.

14. Chris Telley, "The Sinews of Multi-Domain Battle," *RealClearDefense,* retrieved from http://www.realcleardefense.com/articles/2016/12/30/the_sinews_of_multi-domain_battle_110564.html on December 30, 2016.

15. Harry B. Harris, Jr. "Role of Land Forces in Ensuring Access to Shared Domains." Speech given to the AUSA Institute of Land Warfare LANPAC Symposium on May 25, 2016.

16. Eric Lindsey, "Beyond Coast Artillery: Cross-Domain Denial and the Army," *Center for Strategic and Budgetary Assessments.*

17. General Mark Milley, "Remarks at the AUSA Conference 2016," *Association of the United States Army.*

18. Jacquelyn Schneider, "Digitally-Enabled Warfare," *Center for a New American Security,* retrieved from https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox on August 29, 2016.

19. Patrick J. Murphy and Mark A. Milley, "Record Version Statement by The Honorable Patrick J. Murphy, Acting Secretary of the Army, and General Mark A. Milley, Chief of Staff, United States Army, on the Posture of the United States Army" *United States Senate Committee on Armed Services,* April 7, 2016.

20. Perkins.

21. Perkins.

22. Beyerchen.

23. Office of the Secretary of Defense, *The Department of Defense Cyber Strategy,* April 2015, 14.

24. Paul Scharre, "Commanding the Swarm," *War on the Rocks,* retrieved from http://warontherocks.com/2015/03/commanding-the-swarm/ on November 25, 2016.

25. Secretary of Defense Ash Carter, "Remarks on "The Path to an Innovative Future for Defense" *Office of the Secretary of Defense,* October 28, 2016, retrieved from https://www.defense.gov/News/Speeches/Speech-View/Article/990315/remarks-on-the-path-to-an-innovative-future-for-defense-csis-third-offset-strat on December 27, 2016.

NOTES

26. Bob Work, "The Third U.S. Offset Strategy and its Implications for Partners and Allies," speech given at the Willard Hotel in Washington D.C. on January 28TH, 2015, retrieved from https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies on December 29, 2016

27. "Remarks on "The Path to an Innovative Future for Defense."

28. The Path to an Innovative Future for Defense.

29. Formerly Army Cyber's, Cyber Support to Corps and Below, CSCB is now the overarching effort to combine cyber, electronic warfare, and Information Operations to tactical forces. It incorporates support to select rotations to Combat Training Centers that will guide future Army decisions on doctrine, organizational structure, training, materiel, integration, logistics, personnel, and facilities to close known capability gaps across the Army.

30. U.S. Army Cyber Command, "Integration of cyberspace capabilities into tactical units, *Army.mil,* retrieved from https://www.army.mil/article/163156 on November 25, 2016.

31. David Vargan, "Expeditionary cyber aids maneuver commanders," *Army News Service,* r etrieved from http://www.riley.army.mil/News/Article-Display/Article/933299/expeditionary-cyber-aids-maneuver-commanders/ on November 25, 2016.

32. Mark Pomerleau, "What is ISR in non-physical domains?" *C4ISRNET,* retrieved from http://www.c4isrnet.com/articles/what-is-isr-in-non-physical-domains on December 30, 2016.

33. Mark Pomerleau, "How can cyber contribute to multi-domain battle?" *C4ISRNET,* retrieved http://www.c4isrnet.com articles/how-can-cyber-contribute-to-multi-domain-battle on December 27, 2016.

The Cyber Defense Review

◆ Professional Commentary ◆

Clear Thinking About Protecting the Nation in the Cyber Domain*

General (Ret.) Keith B. Alexander (U.S. Army)
Jamil N. Jaffer
Jennifer S. Brunet

The key systems and networks that are colloquially referred to as *cyberspace* constitute a set of critical assets that enable communication, promote economic growth and prosperity, advance the cause of freedom globally, and help ensure US national security and that of our allies. At the same time, cyberspace has become a digital battleground where nation-states and their proxies, organized criminal groups, terrorists, hacktivists, and others seek to gain an advantage over one another, whether through surveillance and espionage, criminal activity, recruitment, planning, and incitement to attacks, and the repression of free speech and expression. Increasingly, the US recognizes that while the benefits of global connectivity far outstrip the potential costs, our increased connectivity also makes us more vulnerable: as individuals, as groups, and as a nation. Today the spread of advanced technologies and the increased connectivity of networked devices to physical systems make it more possible than ever before to create real-world effects through cyber activities. As a result, the US must proactively take steps to protect ourselves, our information, and our critical assets from the vagaries of crime, theft, espionage, and, increasingly, from potentially destructive activities. Unfortunately, as a nation, the US has yet to have the critical conversations and make the decisions necessary to put in place the foundational capabilities necessary to protect the nation in this new domain.

* This article is adapted in part from testimony delivered by General (Ret.) Keith B. Alexander on July 13, 2016 before a combined hearing of two subcommittees of the U.S. House of Representatives Committee on Government Reform and Oversight on Digital Acts of War, testimony delivered by Jamil N. Jaffer before a hearing of the U.S. House of Representative Committee on Small Business on July 6, 2016 on Foreign Cyber Threats, and testimony delivered by General (Ret.) Alexander on November 3, 2015 before a hearing of the U.S. Senate Armed Services Committee on the Future of Warfare.

General (Ret.) Keith B. Alexander is the former Director of the National Security Agency and former Commander, United States Cyber Command. General Alexander currently serves as the President and CEO of IronNet Cybersecurity, a startup technology company headquartered in the Washington, DC metropolitan region.

Technology is an area of rapid and dramatic change and growth, with processing capacity doubling every two years under Moore's law.[1] Indeed, some have suggested that any person with access to Google today has better access to informationthan the President of the United States did fifteen years ago.[2] Others have previously suggested that by 2049, a $1,000 computer will exceed the computational capabilities of the entire human race.[3] The rate of connectivity is increasing rapidly. By 2020, it is expected that IP traffic on global communications networks will reach ninety-five times the volume of the entire global Internet in 2005,[4] and Cisco estimates that by 2020 there will be more than three IP-connected devices per person around the world.[5]

While this expansion of technology and connectivity means that we can expect to reap tremendous social, economic, and political benefits, it also means the attack surface for bad actors to target the US is likewise expanding. From our perspective, there are four major threats in the cyber domain: cyber-attack, cyber espionage, cyber-enabled theft of intellectual property, and criminal activity. In 2014, the Centerfor Strategic and International Studies estimated the worldwide loss from cybercrime to be $445 billion annually.[6] While we are all now well aware of the huge threat posed to our economic security by the rampant theft of intellectual property from American private sector companies by nation-states and their proxies—constituting the greatest transfer of wealth in human history—there is an even more troubling trend that began to take hold in the past four years: the emergence of actual destructive cyberattacks, where cyber or other systems, data, or capabilities are permanently destroyed or disabled.

Jamil N. Jaffer is the former Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee and a former Associate Counsel to President George W. Bush. Mr. Jaffer currently serves as an Adjunct Professor of Law and Director, Homeland & National Security Law Program at the Antonin Scalia Law School at George Mason University and as Vice President for Strategy & Business Development for Iron-Net Cybersecurity.

In 2012, a set of destructive cyberattacks conducted against Saudi Aramco and Qatari Ras Gas disabled over 30,000 computers at Saudi Aramco alone.[7] In February 2014, the US saw the first-ever publicly reported destructive cyberattack by a nation-state on its soil, with Iran attacking the Las Vegas Sands Corporation.[8] This was followed by North Korea's attack on Sony Pictures in November 2014.[9] These attacks represent a particularly concerning trend, as they demonstrate a expansion in cyber activity from nations that are more likely to be unpredictable and dangerous that the typical nation-state attackers with strong capabilities. These attacks also lay bare the fact that the US has no real strategy or doctrine for how to deal with such events, much less deter other nation-states from undertaking them.

To develop such strategies and doctrines, and perhaps most importantly, to effectively deter these type of actions, the US needs to understand better what actions might constitute acts of war in the cyber domain and start putting in place the key elements of a truly defensible national cyber architecture.

When it comes to understanding what might constitute acts of war in cyberspace, it is easy to imagine categories of cyberattacks with consequences that we would likely be prepared to call acts of war. For example, attacks that cause major loss of life, destruction or incapacitation of significant portions of key infrastructure, or even attacks that cause massive economic damage, are likely to cross that line. At the same time, there remains an enormous gray area of hostile nation-state actions that might approach, or may even cross such a line.

In part, the determination of what constitutes an act of war is a legal determination and has legal consequences. International law, including the U.N. Charter, seeks to define when a nation may act in

Jennifer S. Brunet is a former U.S. Air Force defense analyst and staff member of U.S. Cyber Command and the National Security Agency. Ms. Brunet currently serves as an executive staff member at IronNet Cybersecurity.

self-defense and how the international community might respond to a breach of the peace.[10] Similarly, a determination by NATO that a member-state has been attacked could trigger the collective defense commitment in Article V of the NATO Treaty.[11]

At the same time, we cannot ignore the political and moral aspects of determining what constitutes an act of war. Even if a nation suffers an "armed attack" under the U.N. Charter definition, it may choose not to respond. In addition, many argue that the right of self-defense does not require a nation to wait until an armed attack takes place before invoking its right of self-defense against an imminent, pressing threat.[12] Moreover, the decision whether or not to go to war, what constitutes a just cause for war, and how a nation chooses to respond, including the means of warfare it employs, are profoundly moral questions with implications for the overall conduct of war going forward and the ethical constraints we can, and should, apply to ourselves in conducting even a war that is just and legal. These are issues that must be debated, both in the US as well as through international institutions, to assess whether it is possible to develop the beginnings of a reasonable international consensus.

In looking at these questions, particularly in a new domain like cyberspace, the US must think not just about the right and left boundaries of what constitutes an act of war, and how and when to respond, but also about the vital center, and the hard questions that lie within. While there are no detailed answers, it is worth noting that we are not writing on a blank slate; many have considered the implications for just war theory and international law of new domains or new methods of warfare before, whether during the advent of air warfare or the development (and use) of nuclear weapons.[13]

Perhaps even more importantly, we are not even writing on a blank slate when it comes to cyberspace itself. The Tallinn Manual, a NATO-sponsored effort, provides helpful guidance in this area,[14] and will likely continue to do in coming years, as it is being updated in February 2017.

When it comes to adversary activities in cyberspace—whether such activities rise to the level of an act of war or not—it is worth considering how the US might best defend itself against such activities. Today, America's enemies need not attack our government to have a substantive national strategic effect. Indeed, in some ways, attacking the US civilian or economic infrastructure may be a more effective approach in the modern era, particularly for asymmetric actors or nation-state proxies. The future of warfare is here, and we need to understand how to architect the US for this new reality.

One of the key issues the US must address, in creating defensible national cyber architecture, is determining where to place responsibility for the cyber defense of the nation, including its key infrastructures and economic sectors. Today, the basic expectation is that the private sector is responsible for defending itself in cyberspace regardless of the enemy, the scale of the attack, or the type of capabilities employed. While this is the norm today, we must consider whether such an approach continues to make sense going forward, particularly when it comes to nation-state attacks.

The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks. For example, we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD.[15] Today, however, in cyberspace, that expectation is flipped on its head.

> The future of warfare is here, and we need to understand how to architect the US for this new reality.

Some argue that private sector entities should be authorized to 'hack back' or to respond to breaches in an affirmative matter. While this may be a tempting option at first blush, the reality is that authorizing such action could have significant downstream consequences. Offensive actions against a nation-state adversary in cyberspace, regardless of who takes them, could potentially lead to real-world, physical consequences. In most cases, a private entity responding to a nation-state attack will not likely bear the cost of its response. Moreover, in the case of a nation-state attacker, there is also significant potential for a mistake—whether in the scope of the response or with attribution. It is, therefore, no surprise that, at least as a historical matter, we typically assign responsibility for offensive actions to the government, putting such decision-making in the hands of our elected political leaders, not private sector entities or CEOs.

In 2014, then Secretary of Defense Leon Panetta made it clear that US government policy was that "the Department [of Defense] has a responsibility not only to defend DoD's networks but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[16] The reality is, however, that U.S. Cyber Command (USCYBERCOM) does not today have necessary authorities, rules of engagement, and visibility to effectively defend even the federal government itself, much less the whole of the US private sector.[17] The newly elected President should, therefore, work to provide the authorities and rules of engagement necessary to defend at least the government to USCYBERCOM and begin architecting the government's systems to provide the necessary visibility that such a defensive capability would require. This assignment of responsibility and authority ought then be followed by a period of training and exercising of these authorities and capabilities to demonstrate USCYBECOM's readiness and ability to respond to threats at network speed, as appropriate.

The US must recognize that sharing and collaboration are not the end, but rather are a means to a more capable national cyber defense.

It is also worth noting that even if USCYBERCOM had the authority necessary to defend the nation writ large, yet another challenge is that, today as a general matter, the government (and in particular the DoD), lacks the relationships and technological fabric between itself and the private sector necessary to make such authority effective.

This latter point is perhaps the most important one. Neither the government nor the private sector can properly protect the relevant systems and networks without extensive and close cooperation. This is true, in large part, because of the way these systems matured and interacted over the past 20 to 30 years. In particular, the private sector controls a vast majority of the cyberspace real estate, particularly when it comes to critical infrastructure and key resources,[18] which means that to create a truly defensible cyber architecture for the nation as a whole, the government and the private sector must closely collaborate.

To do so, we must fundamentally rethink how the government and the private sector relate to one another in cyberspace. We need to draw clear lines and make explicit certain responsibilities, capabilities, and authorities. Given that a key principle of attack is to aim at the seams of command and control, clearly defined rules, including identifying areas of overlapping responsibility, will help minimize opportunities for a cyberattack.

At the same time, the US must recognize that while creating and assigning responsibilities is necessary to address these challenges, it is not sufficient. The US government must collaborate with private entities to help provide the most effective defense. We must learn how to work together in a cooperative environment, and confront the threats the nation faces. Just as the modern military has learned, over the past three decades, how to train, exercise, operate, and fight in a joint, combined arms environment, so too today must the US public and private sectors learn how to train, exercise, and operate cooperatively in cyberspace.

Initially, the government should partner with the private sector to share both government and private threat information, in real time, at network speed, and in a manner that it can be actioned rapidly. Building out a crosscutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to air traffic control. Just as the air traffic control picture ensures aviation safety and synchronizes government and civil aviation, a cyber common operational picture can synchronize a common cyber defense for the US and its allies, drive decision-making, and enable rapid response.

> The US must stay ahead of the problem, think clearly about the challenges we face, and effectively make the critical decisions that are before us today.

Operating collaboratively also means increased side-by-side interaction in the prelude to a crisis, including cooperative training and exercises. As difficult as it was to convince US armed forces to truly adopt 'jointness' and fight as one force, it will be even more difficult to make the private sector and the government interoperable and capable of performing as single, cooperative unit. However, as with the various military agencies in the post-Goldwater-Nichols era, if the nation's cyber architecture is going to be truly defensible in our increasingly networked and vulnerable world, private sector companies must learn how to work with one another in crisis mode, as well as with the government. This will require some measure of interoperability, common practices and procedures, the ability to quickly and tightly integrate, and, perhaps most importantly, a core level of trust.

At the same time, the US must also recognize that sharing and collaboration are not the end, but rather are a means to a more capable national cyber defense. Sharing and collaborating is essential, but taking action and having the capability and authority to act in appropriate circumstances is critical.

The US therefore also needs to build a complementary foundation within the DoD and must put the right rules, procedures, and structures in place within the larger defense and intelligence communities. In recent years, the government successfully established

USCYBERCOM and brought a joint, combined arms approach to this problem. We must now go further by elevating USCYBERCOM to a Unified Command as directed in the FY 2017 National Defense Authorization Act signed by President Obama this past December, providing a consistent and increased set of funding authorities, developing clear authorities and rules of engagement for the defense of the nation, and investing in both people and technology enhancements, thus preparing for what is a more dangerous and rapidly changing environment.

At the same time, important progress already made ought not to be reversed. The way we intend to operate in cyberspace should define the way we are organized. Moreover, it also means that the cyber investments the government makes should continue to be analogous to and undertaken with the vigor and focus of the Manhattan Project, and ought to involve government, academic, and industry participants.

The situation we have faced in recent years—with a fundamental lack of clear thinking about these problems—is particularly troubling because the reality is that adversaries will not wait for us to get this right. The US cannot rely on a false sense of security; while our systems today are resilient and we are working harder to make them more so, we can and must do more now. Assuming blithely that the private sector or the government standing alone will be able to defend the nation is tantamount to the French reliance on the Maginot Line before World War II.

The US ought not to repeat that historically catastrophic mistake in this new domain of cyberspace. The US must stay ahead of the problem, think clearly about the challenges we face, and effectively make the critical decisions that are before us today—in a time of relative calm and before a major incident. If we fail to do so, we will have no one to blame but ourselves when that day arrives, as it inevitably will.

NOTES

[1] Annie Sneed, *Moore's Law Keeps Going, Defying Expectations,* Scientific American (May 14, 2015) available online at http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/.

[2] Peter Diamandis, *The Future is Brighter Than You Think,* CNN (May 6, 2012) ("Right now, a Maasai warrior on a mobile phone in the middle of Kenya has better mobile communications than the president did 25 years ago. If he's on a smart phone using Google, he has access to more information than the U.S. president did just 15 years ago.").

[3] Ray Kurzweil, *The Law of Accelerating Returns* (March 7, 2001), *available online* at http://www.kurzweilai.net/the-law-of-accelerating-returns.

[4] Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, *available online* at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf; *see also* Cisco, *VNI Complete Forecasts Highlights Tool, available online* at http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html.

[5] *Zettabyte Era,* n. 4 *supra* at 2.

[6] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (May 2014), *available online* at http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[7] Director of National Intelligence James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community 2013* at 1, Senate Select Committee on Intelligence (Mar. 12, 2013), *available online* at https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf; Kim Zetter, *Qatari Gas Company Hit With Virus in Wave of Attacks on Energy Companies* (Aug. 30, 2012), *available online* at https://www.wired.com/2012/08/hack-attack-strikes-rasgas/.

[8] Director of National Intelligence James R. Clapper, *Opening Statement to Worldwide Threat Assessment Hearing,* Senate Armed Services Committee (Feb. 26, 2015), *available online* at https://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf ("2014 saw, for the first-time, destructive cyberattacks carried out on U.S. soil by nation state entities, marked first by the Iranian attack on the Las Vegas Sands Casino a year ago this month and the North Korean attack against Sony in November. Although both of these nations have lesser technical capabilities in comparison to Russia and China, these destructive attacks demonstrate that Iran and North Korea are motivated and unpredictable cyber actors.")

[9] Ibid.

[10] United Nations, *U.N. Charter* Ch. 7, Arts. 39, 41, 42 51, *available online* at http://www.un.org/en/sections/un-charter/un-charter-full-text/index.html.

[11] North Atlantic Treaty Organization, *Wales Summit Declaration* (Sept. 5, 2014), *available online* at http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber; North Atlantic Treaty Organization, *North Atlantic Treaty,* Arts. 4-5, *available online* at http://www.nato.int/cps/en/natolive/official_texts_17120.htm; see also North Atlantic Treaty Organization, *Cyber Defence Pledge* (July 8, 2016), *available online* at http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

[12] White House, *The National Security Strategy of the United States of America* (Sept. 2002), *available online* at http://www.state.gov/documents/organization/63562.pdf; Brian Egan, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign* (Apr. 4, 2016), *available online* at https://www.justsecurity.org/wp-content/uploads/2016/04/Egan-ASIL-speech.pdf.

[13] W. Hays Parks, *Air War and the Law of War,* 32 A.F. L. Rev. 1 (1990); Jill M. Sheldon, *Note: Nuclear Weapons and the Laws of War: Does Customary International Law Prohibit the use of Nuclear Weapons in all Circumstances?,* 20 Fordham Int'l

L.J. 181 (1996) (collecting materials).

[14] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), available online* at https://ccdcoe.org/tallinn-manual.html.

NOTES

15. Department of Defense, About *USNORTHCOM, available online* at http://www.northcom.mil/About-USNORTHCOM/ ("USNORTHCOM partners to conduct homeland defense, civil support and security cooperation to defend and secure the United States and its interests. USNORTHCOM's AOR includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles."); Department of Defense, *North American Aerospace Defense Command* (Apr. 25, 2013), *available online* at http://www.norad.mil/Newsroom/Fact-Sheets/Article-View/Article/578770/north-american-aerospace-defense-command/ ("The North American Aerospace Defense Command (NORAD) is a United States and Canada bi-national organization charged with the missions of aerospace warning and aerospace control for North America. Aerospace warning includes the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, through mutual support arrangements with other commands. Aerospace control includes ensuring air sovereignty and air defense of the airspace of Canada and the United States.").

16. Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (Oct. 11, 2012), *available online* at http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

17. See General Accountability Office, *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents* at 12 (Apr. 2016) ("We found that DOD guidance…does not clearly define the roles and responsibilities of key DOD entities…if they are requested to support civil authorities in a cyber incident…Further, we found that, in some cases, DOD guidance…does not provide the same level of detail or assign roles and responsibilities for cyber support. In other cases, the designation of cyber roles and responsibilities in DOD guidance is inconsistent."); *id.* at 20 ("[T]he absence of clarity in roles and responsibilities to address a cyber incident represents a clear gap in guidance. The gap, and the uncertainty that results, could hinder the timeliness or effectiveness of critical DOD support to civil authorities during cyber-related emergencies that DOD must be prepared to provide…[W]ithout clarifying guidance on DOD roles and responsibilities in a cyber incident, DOD cannot reasonably ensure that the department will be able to most effectively employ its capabilities to support civil authorities in a cyber incident."); *see also* Department of Defense, *The DOD Cyber Strategy* at 7 (Apr. 2015), *available online* at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf ("For example, DoD's own network is a patchwork of thousands of networks across the globe, and DoD lacks the visibility and organizational structure required to defend its diffuse networks effectively.").

18. Office of the Director of National Intelligence, *Office of the Program Manager-Information Sharing Environment, Critical Infrastructure and Key Resources, available online* at https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

Cybernomics – Changing the Economics of Cyber Defense

Snehal Antani
Ravi Iyer

Cyber defense is on an unsustainable trajectory. Thanks to freely distributed and automated attack tools, cheap labor in countries from which attacks are launched, and stolen computing resources assembled into botnets, the cost of cyber-attack is estimated to be one-tenth to one-one hundredth the total cost of cyber defense.

Despite the increased investment in cyber defense, breaches are still occurring, and organizations are still subjected to financial and reputational risk, moreover, cybersecurity has moved beyond a corporate issue, and is now a national security matter. The emerging national urgency to protect us from cyber-attacks will transform into a movement that will fundamentally alter the economics of the problem. Cyber will become the '*Space Race*' of our generation, and victory will require tremendous collaboration across government, academia, and the private sector.

There are six primary areas of focus needed to shift the economics of cyber defense:

1. ORGANIZATIONS MUST SHIFT LEFT—CATCH SECURITY VULNERABILITIES EARLIER IN THE TECHNOLOGY LIFECYCLE.

Shifting left incorporates the following four key concepts: First is Continuous Delivery, which promotes early and continuous software testing including static and dynamic security analysis tools; Second is Architecture-as-Code, which eliminates *snowflake* systems—manually configured system components that are unique in some way ± through standardization and automation; Third is End-to End Instrumentation connecting the dots across software development, systems deployment, and systems operations; and Fourth is a Continuous Improvement Process that reviews and prioritizes the resolution of Reliability, Availability, Serviceability, and Security (RASS) issues identified by operations. A litmus test for success is when leaders can convey in real time: who are their best/worst developers, best/worst contractors, which developers/contractors are struggling to write secure code. If a developer or contractor is sent off to learn how

Snehal Antani serves as the SVP/GM of Business Analytics & IoT for Splunk. He joined Splunk in 2015 as CTO, where he helped drive the long term vision and strategy for the company across Business Analytics and the Internet of Things. Prior to Splunk, he served as CIO of GE Capital's Distribution Finance business, as well as Chief Architect for GE Capital North America. In 2016, Antani was recognized as a Premier 100 award winner by Computerworld, for the digital transformation he drove while at GE, evolving IT from a back-office function to a core part of the value delivered to customers. Snehal started his career as a software engineer at IBM, where his work led to 11 patents spanning systems optimization, data processing, and large-scale transaction systems. Snehal holds a Bachelor's Degree in Computer Science from Purdue University, and a Master's Degree in Computer Science from Rensselaer Polytechnic Institute (RPI).

to write secure software, IT leaders should see a quantifiable return on that investment of time. That level of data-driven transparency ensures that technology systems are shipped when ready, and not restricted to a date; more importantly, those technology systems are secure by design, versus discovering and trying to remediate issues later in the delivery lifecycle.

2. ORGANIZATIONS MUST HAVE THE RIGHT OPERATIONAL MODEL IN PLACE TO EFFECTIVELY DETECT AND REMEDIATE A VULNERABILITY OR BREACH.

The optimal strategy driving your Security Operations Center (SOC) should be governed by analytics, including critical elements such as quick detection, thorough investigation, and rapid remediation. In addition, the processes that govern how security analysts operate must be frictionless.

Quick Detection relies on the ability to monitor complex IT and security systems for security threats in real-time while providing security practitioners visual insights into that data. The capability to correlate events in near real time while measuring against baseline relationships is key. This enables quick detection by practitioners by identifying previously unknown relationships in messages or events generated by devices, systems or applications, based on characteristics such as the source, target, and protocol or event type.

Thorough investigation requires the ability to correlate real-time data with historical data to examine and determine how harmful, how widespread and how deep within the organization an attack can penetrate. This requires validating against well-known threat intelligence to gain additional context of attacker's tactics, techniques, and procedures (TTPs). Mechanisms that speed up the investigation portion of an alert are critical to fast and thorough security investigations.

Ravi Iyer is the Senior Director, Security Product Management, in Splunk's–Security Markets group. Prior to Splunk, Ravi has held various Engineering, Product Management and Product Marketing positions at startups and blue chip companies. Most recently as SVP of Products at Vorstack/BrightPoint (acquired by ServiceNow), VP of PM/PMM at WhiteHat Security and as Sr. Director of PM at Good Technology (acquired by RIM). Ravi started his career as an engineer for network management products at AT&T–Bell Labs. Following that he was the lead engineer in the Directory Services (LDAP & DNS) group for multiple Solaris releases following which he went on to lead Product Management for Solaris OS at Sun Microsystems. Ravi holds a Bachelor's Degree from Bangalore University and an MS in Computer Science from University of Missouri.

Rapid Response requires customizable workflows that integrate the detection and investigation phases of security operations with the response phase. Typically, this involves providing integration with ticketing systems that assign tasks and monitor the completion of these tasks. Many organizations are embracing automation within their SOC to respond to threats quicker than ever before.

3. ORGANIZATIONS MUST EMPLOY SECURITY ANALYTICS TO MAXIMIZE THREAT HUNTING.

The maturation of machine learning technologies and their ability to detect security threats has significantly enhanced the capabilities of security analysts. When analysts monitor the behavior of users, hosts, and networks, unsupervised machine learning can produce high fidelity alerts for investigation, which reduces the noisy but benign alerts that plague the daily life of security analysts. A tiered strategy is optimal here, where classic machine learning models first identify anomalies, and advanced data science techniques, as well as security threat expertise, are later applied to generate threat models that yield high-fidelity threats.

Employing such data science techniques make it possible to identify remote account takeovers, attacker dwell time, lateral movement with compromised credentials and advanced persistent threats (APT's) such as data exfiltration with malware.

Advanced user-behavior analytics solutions provide a significant additional capability that includes peer group analytics, workflows that enable analyst investigations (hunter-centric), and kill-chain visualization.

4. EXPEDITE INCIDENT RESPONSE BY INTRODUCING AUTOMATION.

By our count in the field, the security vendor portfolio of most organizations is typically made up of more than seventy technologies—an astonishing number. To optimize the investments you are making in these technologies, diverse domain expertise is required across every team. But because we see such a skills shortage in cyber security, the ability to make well-informed decisions quickly remains the biggest and most expensive challenge facing security teams today.

When large teams of different skill sets are brought together to investigate, observe and characterize a threat, the challenge of short-term containment and mitigation combined with long-term policy modification can pose significant challenges. This unprecedented complexity grinds down the efficiency of security operations.

> Cyber will become the *Space Race* of our generation, and victory will require tremendous collaboration across government, academia, and the private sector.

Automating many of these functions can significantly boost operational effectiveness. Efficient security operations typically implement a playbook approach for investigation and remediation of various types of alerts. Analogous to reflexes in the human body, operational effectiveness can be dramatically increased by automating these playbooks, with scale varying depending on the maturity level of your SOC. Organizations lower on the maturity curve may employ only the most basic of security automation, while more mature security operations may employ complex orchestration that forms the basis of multi-step investigation and remediation.

5. ORGANIZATIONS MUST ACCELERATE ANALYST PRODUCTIVITY.

As mentioned above, the security skills gap is a very real thing. Corporations and government agencies struggle mightily to fill cyber defender jobs. In addition to requiring tremendous technical breadth across a myriad of topics including networking, operating systems, and the latest attack vectors, cyber defenders spend the bulk of their time investigating issues across a number of emerging security technologies, which analysts must continue to learn and master.

Each of these technologies has nuanced search languages that require specialized training, which further leads to a scarcity of trained talent and a longer ramp to productivity. To combat all of this, organizations are turning to natural language and advanced visualizations to help accelerate the ramp to productivity for a cyber defender.

Natural language search allows security analysts to ask questions that are more intuitive, e.g., *How many users logged in yesterday,* which is then dynamically transformed into an optimized search and executed against the data. The insights derived can be conveyed through advanced visualizations and data storytelling techniques, enabling the analyst to quickly dissect the data and come up with the next question to ask. Decreasing the required training time to search data and time to synthesize search results accelerates the ramp-to-productivity, enabling organizations to have access to a larger talent pool of cyber defenders.

6. ORGANIZATIONS MUST BECOME A MOVING TARGET TO DISORIENT AND DECEIVE ATTACKERS.

An attacker spends most of their time in reconnaissance mode—studying the network topology and systems architecture of the target to identify angles of attack. There are two key emerging technologies that disrupt an attacker's ability to conduct reconnaissance: shape-shifting networks and deception techniques.

The static nature of systems enables an attacker to attack at their leisure. Shape-shifting networks leverage software-defined networking to dynamically change the network configuration of a system, decreasing the window of attack and increasing the cost to probe. Deception techniques mimic the target system, creating the illusion that an attacker has found an exploited an angle of attack.

Shape-shifting networks, combined with deception techniques, can serve as a powerful solution for dramatically increasing the cost of attack, making it economically unfeasible for a hacker to spend precious time to exploit. This truly turns the economics of a hack in its head.

Shape-shifting networks, combined with deception techniques, can serve as a powerful solution for dramatically increasing the cost of attack.

CONCLUSION

Clearly, organizations have strategies available to them today to shift the balance of cyber economics in their favor. New trends in automation, machine learning, and analytics have created a golden opportunity for organizations to flip Cybernomics in a way that has never been possible before, but changing the economics goes beyond emerging technology, where ecosystem and collaboration across ecosystem members are critical. As organizations take a look at their security landscape in 2017 and beyond, it will be paramount to determine if the strategies outlined above are being embraced to shift the balance of cost from defender to hacker. Moreover, embracing these concepts enables organizations to have the agility of a start-up, with the resources of an enterprise. These organizations can rapidly create new capabilities faster than their competitors or adversaries, and take advantage of opportunities that help drive mission success.

Cyber (In)Security: Decision-Making Dynamics When Moving Out of Your Comfort Zone

Andy Cohen

"Every assumption we hold, every claim, every assertion, every single one of them must be challenged."[1] —General Mark A. Milley, 39TH Chief of Staff of the U.S. Army

OVERVIEW

This paper focuses on how the dynamic speed of change and the compression of time in cybersecurity move individuals and organizations out of their comfort zones. This often results in forcing faulty decision-making generated by an enhanced dependence on untested assumptions. The counterbalance to this behavior begins by recognizing a key truism: within every decision lies an assumption. Equipping your cyber team with the mechanisms and tools to identify and properly challenge these assumptions drives better decision-making and new opportunities to successfully defend, attack, and adapt in the cyber battleground.

Making Decisions Outside Your Comfort Zone

Aron Ralston, the hiker forced to sever his own arm after it became stuck between two rocks and the inspiration for the film *127 Hours*, admitted that his greatest fear throughout the entire ordeal was having to get a shot at the hospital. Needles made him uncomfortable.[2]

Orville Wright, one of the two brothers who ushered in the art of modern aviation by inventing and flying the first plane, dismissed the idea of creating a runway that smoothed over the rocks and debris on the airfield. In his eyes, if a man had to smooth over every takeoff strip (which today is called a tarmac), he shouldn't be flying. Investing in a tarmac seemed silly to him.[3]

Houdini was the king of escapes—nothing could hold him back. Yet when riding with a friend in a new car, he couldn't open the door on his own because the door handle was in a different place than the one on older models. Joked Houdini, "I've escaped from practically every type of a container and every size, shape, and weight of boxes, trunks, and other such things, but I wish someone would tell me how I can get out of this darned automobile!" [4] One simple design change had stymied the master.

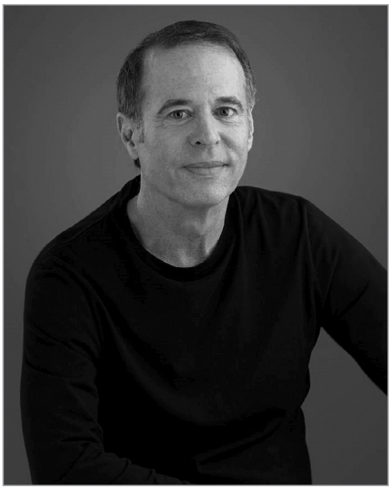
These three examples demonstrate that even people who have built their reputations on doing things differently often make faulty or irrational decisions when moving out of the security of their comfort zones. And as Ralston, Wright, and Houdini demonstrate, it has nothing to do with courage, IQ, talent, or success.

What's Your Cyber Comfort Zone?

Scott Scheferman is a hacker turned Director of Consulting for Cylance, a cybersecurity consulting firm incorporating artificial intelligence. In a popular blog post titled *Ransomware Predictions Past, Present, Future,* he wrote: "As individuals and as a collective society, we are basically novices when it comes to understanding cyber risks, being able to identify an attack, and preparing ourselves for a compromise." [5]

This observation doesn't dismiss the value of cyber talent or years in the field. Rather, it reminds us that in cybersecurity, the number of unknowns is significantly higher than the knowns, regardless of experience and expertise.

Verizon's *2016 Data Breach Investigations Report* provides a powerful metaphor for battling these unknowns. The report asks you to imagine that a "soldier is told to guard a certain hill and keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike." [6] This metaphor plays out every day in the corporate world. Millions of dollars are invested in protecting against illegal entry into an organization's server,



Andy Cohen is an entrepreneur, best-selling author, and international thought leader. His keynotes and workshops are world-renowned and include appearances at the Army Cyber Institute, Google, HSBC China, and The World Bank. He has a degree in experimental psychology and a room full of prestigious advertising awards for finding creative solutions that drive measurable sales. Andy is the Chief Assumption Officer of Andy Cohen Worldwide, a global advisory firm helping multinational businesses as well as small firms make faster, better decisions. Between engagements, Andy teaches at the world's most respected universities including New York University, Duke University's Fuqua School of Business, UC Berkeley, ISB (India), and CKGSB (China). *Follow the Other Hand,* Andy's first book, was a *New York Times* notable book. It has been translated into multiple languages. Colonel (Ret.) Greg Conti, Ph.D. called Andy's newest book, *Challenge Your Assumptions, Change Your World,* a must-read for the security professional."

yet the real threat may turn out to be a trusted employee. The scenario goes like this. Hackers identify an employee as a target and exploit that employee's vulnerability with malware or code, giving the hacker access to the C: drive or PC. The data at risk is then encrypted and becomes ransomware. If the company wants that data back, they must pay for it. In other words, the hackers, through phishing or social media, trick the employee into clicking a link and letting ransomware bypass every one of those expensive server protections. In cybersecurity, you constantly confront daily unknowns and rarely know what tomorrow may bring.

Moving out of your comfort zone requires a level of openness to considering new ideas and solutions rather than reverting to old, comfortable ways of doing things. For example, today's military leaders, more comfortable fighting tactical battles on the ground, face tough decisions because they are engaging in unfamiliar battles taking place only in space and time.

> People who have built their reputations on doing things differently often make faulty or irrational decisions when moving out of the security of their comfort zones.

So how do you see things for what they are or are not when the cyber battlefield is constantly shifting in time and space with an enemy that is often invisible? How do you fight when there are no rules to follow because what happened in the past has no definitive relationship to what will happen in the future?

Answers begin with taking a contrarian viewpoint: making an assumption is neither good nor bad because within every decision lies an assumption.

Leveraging Your Assumptions for Better Decision-Making

The late Chris Argyris, management guru, father of "organizational learning," and professor at Harvard Business School,[7] illuminated the "invisible process" that formulates our thoughts leading to decisions. He created a mind map illustrating how we think called the Ladder of Inference.[8] Look at the diagram in Figure 1, and you will see that our thought process is like a ladder—each rung has a purpose.

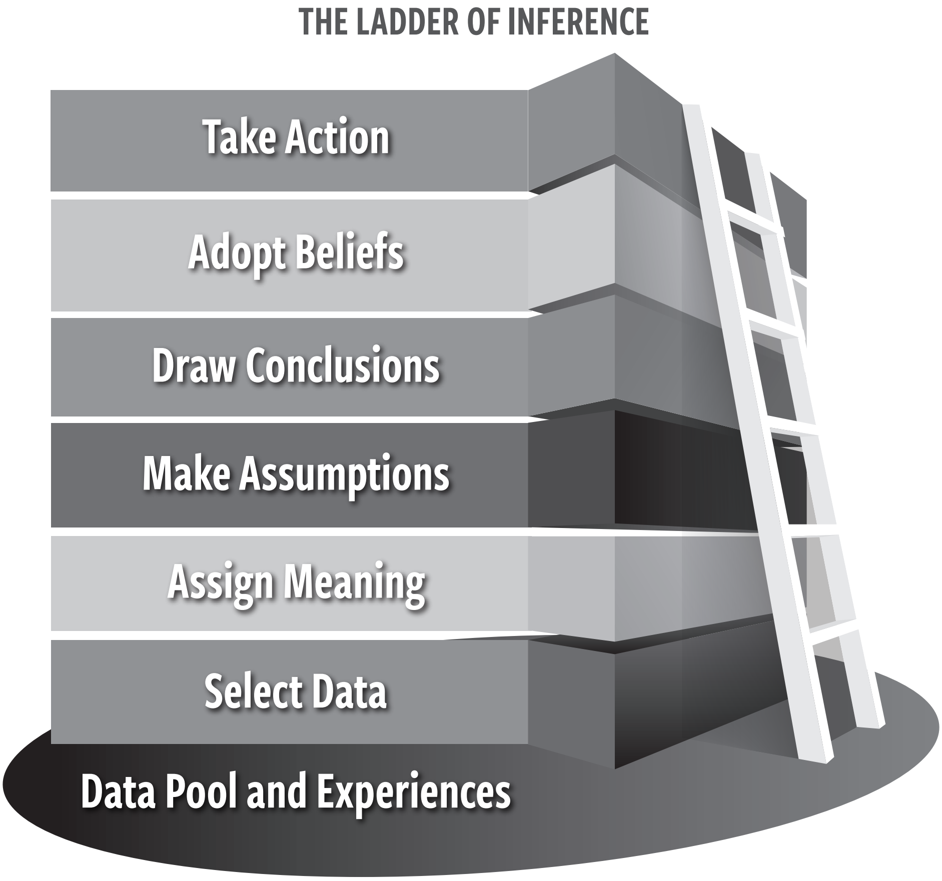


Figure 1. The Ladder of Inference. A mind map created by the late Chris Argyris.

You begin by collecting data, then sorting through that data to form your assumptions. From there, you draw an inference, making a decision that leads you to an action. It's a simple and linear process that explains much about our behavior. This is why the Ladder of Inference is so highly respected in the field of learning and development as an instructive metaphor to explain the decision-making process influencing your actions. The Ladder serves multiple purposes by helping you become more aware of your thinking, making that thinking visible and providing a way to probe what others are thinking. Understanding your "true thoughts" leads to smarter decisions. This does not diminish the value of trusting your "gut." However, there are too many decisions to make in the course of just one day, and trusting your instincts alone isn't enough to help you manage these decisions.

The Ladder illustrates that the middle rung of every decision is the assumption. The assumption is something you treat as a truth rather than simply believe; it is something taken for granted, often subconsciously.

In working with the U.S. Army, I discovered that unlike most organizations, the military very specifically addresses the assumption's role in the decision-making process. Its definition of assumption is "a supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action."[9] At the same time, I observed that the process of identifying and then challenging assumptions is not always personally internalized. As one military leader confided, "Most [in the military] recognize the importance of assumptions but don't often invest enough time in developing them."

The reason to make this "investment" is that the assumption is one of the key components behind every action. The meaning of this is significant—that is, making an assumption is as natural as breathing. To judge yourself for making an assumption is unproductive: don't be held back by blaming yourself for an action that is a natural part of the decision-making process. Instead, accept that you make assumptions by surfacing them and owning them without guilt. The process of doing this is called *making an Assumpt!,* and we will explore this process in greater detail further on. What is important to note right now is that once you make an Assumpt!, you have the power to decide if you want to invest in that assumption or challenge it.

Managing Your Assumptions Outside of Your Comfort Zone

Moving out of your comfort zone produces anxiety—approving a cyber budget might elicit the fear of failure; learning to think like the enemy might force you to consider the inconceivable; changing the way you command a team that operates better without directive leadership may drive you crazy; facing a ransomware experience may generate sheer panic as you lose everything unless you pay.

> Learning to think like the enemy might force you to consider the inconceivable.

Regardless of the situation, Figure 2 suggests that there are also a number of assumptions generated when moving out of your comfort zone. These assumptions are quickly propagated for a number of reasons: fear, change, facing a new experience or confronting the inconceivable. Many of these assumptions serve the purpose of gently coaxing you back into your comfort zone as a way to reduce that anxiety. In other words, they act as barriers to new thinking or solutions. They are *dangerous.*

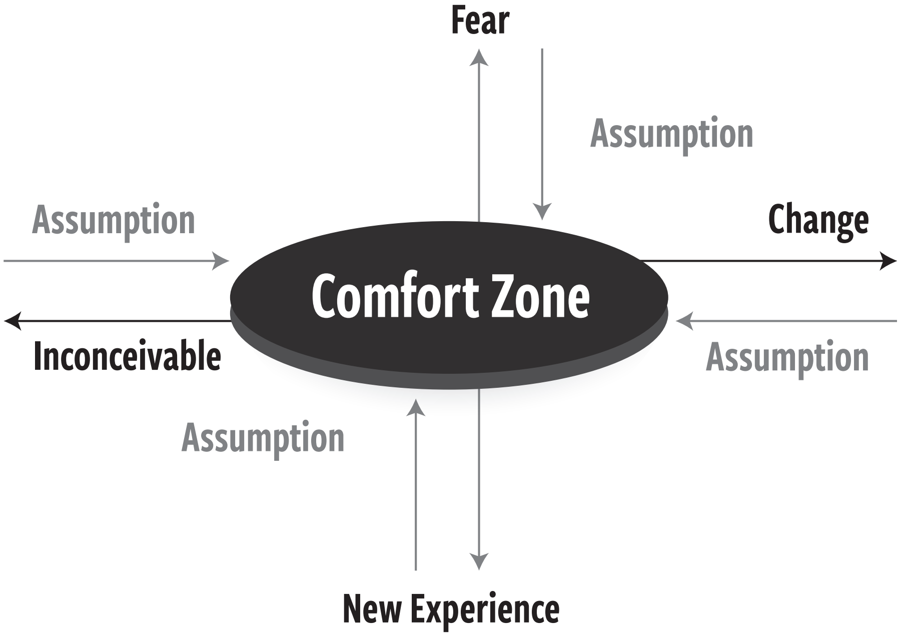


Figure 2. Assumptions push you back into your comfort zone.

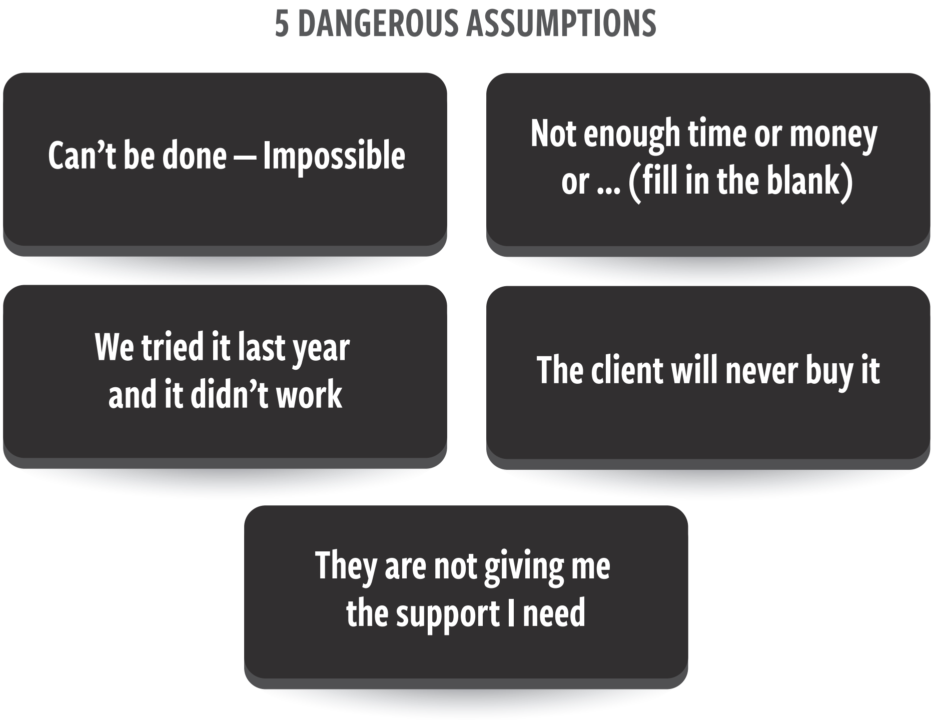
For example, Micah Zenko's comprehensive book *Red Team: How to Succeed by Thinking Like the Enemy* provides a structured process that "seek[s] to better understand the interests, intentions, and capabilities of institutions or potential competitors" through "simulations, vulnerability probes, and alternative analyses."[10] The author points out that often leaders undermine the red team's goal. They fear that the exercise may uncover a leadership weakness (which is part of the purpose of the exercise) that will reflect on them (which it will). When presented with a red team proposal, a leader may point out that a red team exercise was tried a year before without results. This is a dangerous assumption to invest in on face value. Last year, a number of things could have gone wrong such as the structure not being properly set up. Or it may have gone right, and the red team didn't find any issues. The point is, what worked or didn't work last year is, on the surface, no yardstick of future success. "It didn't work last year" is a cue that an assumption is being played out as a reaction to change.

"It worked last year, so let's do it again" is also a verbal cue that an assumption is being made. In the late 1700s, a trusted Dutch military strategy for defending against the French was to flood low-lying areas, separating them from the invaders. This unique system, called *waterlinie,* had proved an effective defense for over two hundred years and through multiple wars. The Dutch *waterlinie* was designed to be deep enough to prevent walking through yet shallow enough to inhibit boating. In 1794 and 1795, however, the weather was extremely cold, and the water froze over, giving the advantage to the French who crossed the ice and won the battle.[11]

“Preparing for the last war” assumes that what worked before will work again, and the phrase serves as a strong reminder of the value in surfacing key assumptions.

A good question to ask at this point is, “How do you recognize most assumptions if they are made subconsciously?” There is no one answer to this question, but a fast solution, as mentioned before, is to listen to what you and others are saying in response to thinking differently and making a change.

You can often recognize these assumptions via verbal cues as in Figure 3.



5 DANGEROUS ASSUMPTIONS

Can’t be done – Impossible

Not enough time or money or ... (fill in the blank)

We tried it last year and it didn’t work

The client will never buy it

They are not giving me the support I need

Figure 3. Verbal cues to unlock dangerous assumptions.

Over time I have collected a number of these verbal cues from all walks of business and put them into a database called the Dangerous Assumptions Database (DAD). The DAD’s nomenclature pays homage to a famous leadership quote that “assumptions are the MOTHER of all screw-ups.” The DAD help you identify these MOTHERS and then quickly identify certain beliefs that we treat as truths.

These include:

- "I'd never do it that way." (Thinking that the world thinks like you)
- "We are smarter than our enemy." (Believing that you and your team are the best)
- "This is good code." (Wanting to believe that the source code run through the compiler translates without flaws)
- "No one would ever do that." (Thinking that if you can't imagine doing something, others won't imagine doing it as well)

I have been collecting dangerous assumptions for years and am happy to share part of this database if you follow up with me at andy@andycohen.com. Once you enhance your ability to "listen" for assumptions, the next step is deciding how to manage them when out of your comfort zone. Let's look at an example in weapons building.

Building a Weapon Outside the Comfort Zone

General Mark A. Milley, four-star general and 39TH Chief of Staff of the U.S. Army, has been providing a wake-up call that encourages the Army to move out of its comfort zone and rethink how future wars will be fought and won. "Rapid change has become increasingly compressed," he said in a speech at the 2016 Association of the U.S. Army Annual Meeting and Exposition's Eisenhower Luncheon. "Those of us today will find it difficult to recognize the battlefield of 2035, let alone 2050 … Crisis will unfold rapidly, compressing decision cycles and response times. Ambiguous actors, intense information wars, and cutting-edge technology will confuse situational understanding." [12]

This means the Soldier on the ground may often be operating solo, cut off from any form of communications with headquarters and peers, and must never stay in the same place past an hour or two in order to escape detection. General Milley describes a scenario in which the independent Soldier will have the ability to replace a weapon part on demand via a portable 3D printer. [13]

In light of these changes, General Milley also questions today's process to acquire and build future weapons. He suggests that the Army revisit the process, streamlining the timeline to address changing technology and the critical need for speed. [14]

Creating Cyber Weapons

Major James Twist is a lead analyst at the Army Cyber Institute at West Point and picks up on General Milley's message. In his lectures, he often shows a DoD acquisition and technology flowchart to demonstrate the complexity of acquiring a new weapon, such as a rifle, onto the battlefield. Figure 4 represents just a small portion of the chart yet clearly illustrates the number of levels, steps, and processes involved in integrating a weapon into the military.

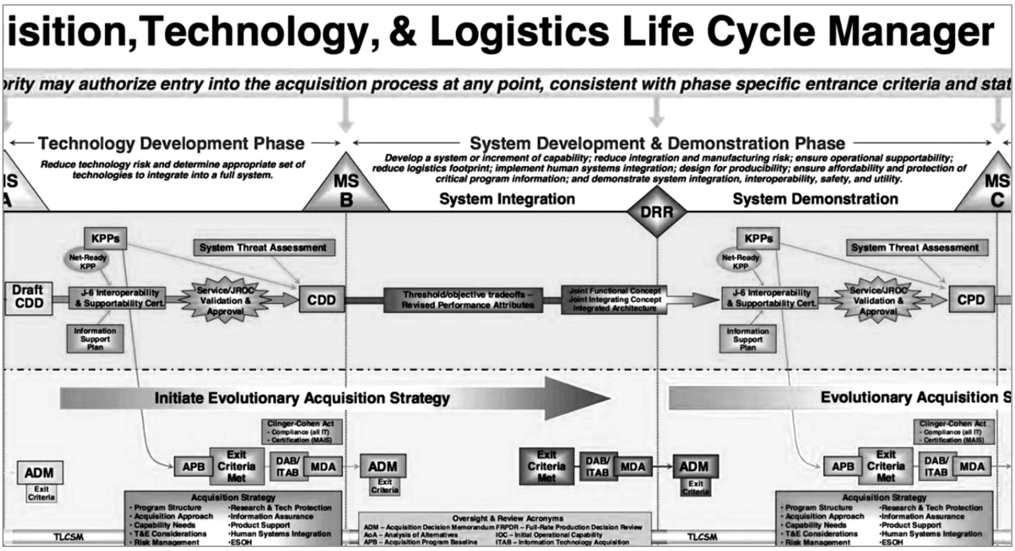

isition,Technology, & Logistics Life Cycle Manager
rity may authorize entry into the acquisition process at any point, consistent with phase specific entrance criteria and stat
Technology Development Phase
Reduce technology risk and determine appropriate set of technologies to integrate into a full system.
System Development & Demonstration Phase
Develop a system or increment of capability; reduce integration and manufacturing risk; ensure operational supportability; reduce logistics footprint; implement human systems integration; design for producibility; ensure affordability and protection of critical program information; and demonstrate system integration, interoperability, safety, and utility.
IS A
MS B
System Integration
DRR
System Demonstration
MS C
KPPs
Net-Ready KPP
System Threat Assessment
Draft CDD
J-6 Interoperability & Supportability Cert.
Service/JROC Validation & Approval
CDD
Information Support Plan
Threshold/objective tradeoffs – Revised Performance Attributes
Joint Functional Concept
Joint Integrating Concept
Integrated Architecture
KPPs
Net-Ready KPP
System Threat Assessment
J-6 Interoperability & Supportability Cert.
Service/JROC Validation & Approval
CPD
Information Support Plan
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition S
Clinger-Cohen Act
- Compliance (all IT)
- Certification (MAIS)
ADM
Exit Criteria
APB
Exit Criteria Met
DAB/ ITAB
MDA
ADM
Exit Criteria
Exit Criteria Met
DAB/ ITAB
MDA
ADM
Exit Criteria
Clinger-Cohen Act
- Compliance (all IT)
- Certification (MAIS)
APB
Exit Criteria Met
DAB/ ITAB
MDA
Acquisition Strategy
· Program Structure
· Acquisition Approach
· Capability Needs
· T&E Considerations
· Risk Management
·Research & Tech Protection
·Information Assurance
·Product Support
·Human Systems Integration
·ESOH
Oversight & Review Acronyms
ADM – Acquisition Decision Memorandum
AoA – Analysis of Alternatives
APB – Acquisition Program Baseline
FRPDR – Full-Rate Production Decision Review
IOC – Initial Operational Capability
ITAB – Information Technology Acquisition
TLCSM
TLCSM
Acquisition Strategy
· Program Structure
· Acquisition Approach
· Capability Needs
· T&E Considerations
· Risk Management
·Research & Tech Protection
·Information Assurance
·Product Support
·Human Systems Integration
·ESOH

Figure 4. A portion of the DoD acquisition and technology flowchart.[15]

The challenge of working within this flowchart is that by the time the new technology (code, piece of software, digital listening device, new gear, etc.) gets processed and approved, the technology involved is already outdated.

A small team at General Motors (GM) faced a similar challenge when tasked with creating a telemetric system for future cars called *OnStar.* Nick Pudar, now Director of Strategic Initiatives at GM, tells the story of when he joined the *OnStar* team:

> In the early nineties, Rick Wagoner, then the president of GM North America, believed that the future of the auto industry went beyond fast, efficiently run, and comfortable cars and chose an *effect:* developing a new type of communications system for the car. The overall obstacles in launching this kind of product were significant. At the time *OnStar* was conceived, the typical total life cycle of a vehicle program was eight to ten years. It took two years to create the product, two years to test and integrate it into the manufacturing processes, and then four to six years of having the hardware built into the vehicles as part of the regular production run. Heavily integrated technologies such as the electronics represented by *OnStar* traditionally would need to wait many years for the next major redesign of the total vehicle. Only then would you see opportunities to implement major improvements. In contrast, the average electronic product development cycle, like *OnStar* technology, was eighteen months. It was initially assumed that these two product cycles were incompatible.[16]

So the first thing GM had to do was move out of its comfort zone by acknowledging this assumption and assessing if it was true or just a set of beliefs. Even Chet Huber, who was there in the beginning and became president of *OnStar*, said that it would have been easy to walk away from the project. Nobody really wanted to challenge the assumption of the accepted production practice.

Preparing for the last war assumes that what worked before will work again, and the phrase serves as a strong reminder of the value in surfacing key assumptions.

"Luckily, someone did," said Pudar. "Rick Wagoner empowered the team to 'follow the other hand' [by challenging their assumptions]." This allowed the team to "simply break all the product development rules, and through diligent engineering, study and identify the absolute latest integration point in the existing processes." [17] In essence, the team rejected the assumption that they had to fit an eighteen-month electronic product development cycle with an eight-year vehicle development cycle and focused on the opposite—fitting a lengthy production cycle into a shorter technology cycle.

That was in 1997. *OnStar* continued to test this assumption; within five years of the launch, they had instituted eight generations of technology updates. [18] Less than twenty years later, *OnStar* reported a subscriber base of over 7 million with more than 1 billion interactions. [19]

The willingness of GM to move out of its design and production comfort zone and challenge traditional assumptions proved beneficial in building a new business and staying ahead of the competition. The story illustrates that the Army needs to move out of its comfort zone and consider building a cyber weapon acquisition process centered on the technology rather than the other way around.

The Dark Web's Role in Cybersecurity

Once you give yourself permission to identify your assumptions, you open the door to a journey that takes you down multiple paths, leading to new opportunities and solutions. For example, rather than spend hours trying to streamline the process to acquire valuable data to use as a weapon, why not create a new channel? Instead of spending two months outsourcing the creation of an expensive code, go directly to the Dark Web. The Dark Web is considered an anonymous cyberspace where at least half of its visitors are selling illegal information, data, codes, drugs, pornography, and weapons.

Military leaders may dismiss the concept of purchasing illegal data as a nonnegotiable as it conflicts with the Army's moral code. This author can only suggest that "buying on the Dark Web" is an assumption to be recognized and then explored, rather than accepted. Major Twist suggests testing the viability of purchasing Dark Web data in order to explore the pluses and negatives as a cyber strategy for acquiring key information.[20]

Many key cybersecurity decisions are based on a risk/reward basis. For some companies, it's financially prudent to pay for the cost of an attack rather than invest unknown dollars in preventing one. What undermines the risk/reward ratio is the assumption of understanding the price of data. How much is a personal social security number or credit card actually worth to an illegal buyer? How much money will an attacker ask for to release a piece of ransomware? This information is important when determining a risk-to-reward cybersecurity strategy to protect data vulnerabilities. You might assume a specific piece of information is worth 75 cents when on the Dark Web it could sell for $1.25 or 25 cents. Either way, you are operating under a giant assumption around value instead of validating it in a real Dark Web setting where this data is sold or through insurance companies, like CyberPolicy.com, which protect against cyberattacks.

Discussions challenging accepted assumptions raise other important issues as well. For example, the Army is committed to recruiting top talent in cybersecurity. This means having to consider a software engineer who might have used drugs. Presently, this is unacceptable under Army requirement guidelines. But to see this as a *rule forever* rather than a present operative assumption hinders the discussion of how to build the best cyber team for the Army.

The Value in Thinking Like the Enemy

In the movie *Star Trek II: The Wrath of Khan* (1982), Captain James T. Kirk, played by William Shatner, reveals his character when he faces a Kobayashi Maru scenario in the form of a computer simulation where the commander of the ship can never win. The simulation occurs when he is a young cadet and ordered to save a stranded spaceship disabled in enemy territory. But that's where the no-win scenario unfolds: it's actually a trap. So saving the ship means the destruction of his spacecraft, but choosing not to mount the rescue mission will result in the destruction of the stranded spaceship.

Captain Kirk, however, beats the program by hacking into the system and rewriting the program before he faces the simulation, thus ensuring he will win.[21] In a much later release, *Star Trek* (2009), Kirk, played by Chris Pine, is initially accused of "cheating" but is later awarded a special citation by the Starfleet Academy for "thinking differently" about confronting the overall challenge.[22]

It's easy to assume that a fictitious concept has little relevance for today's cyber issues. James L. Caroland, an adjunct associate professor in the University of Maryland University

College's Cybersecurity Program, and retired Colonel Gregory Conti, former director of the Army Cyber Institute and associate professor in the United States Military Academy's Department of Electrical Engineering and Computer Science, would argue differently.

The pair performed a fascinating experiment designed to help students of cybersecurity think differently by giving them a seemingly "impossible" task.[23] Students needed to solve a problem that required memorization but whose answer could not be memorized. The only solution was to cheat, and their grade was dependent on their level of creativity in finding a way to do so. Put another way; students faced their own Kobayashi Maru: they had to cheat to pass the test.

> The Army needs to move out of its comfort zone and consider building a cyber acquisition process centered on the technology rather than the other way around.

But the teachers had another catch: if students got caught cheating, they would fail. Students' solutions were both amusing and impressive. One student used his Mandarin Chinese skills to hide the answers. Another put the answer on a soda can, which could be turned away from the proctor as he walked by. The winning student used a false book cover in which the answer was coded on the back cover.

The premise behind this exercise was that "cheating will challenge students' assumptions about security and the trust models they envision."[24] According to the professors of the course, it is through "learning the thought processes of our adversaries that we can hope to unleash the creative thinking needed to build the best secure systems, become effective at red teaming and penetration testing, defend against attacks, and conduct ethical hacking activities."[25]

The purpose of this research was to help these students become more responsible in this field. According to the professors, "By anticipating such actions and reactions, ethical actors are far better prepared to build secure systems and perform both defensive and offensive activities successfully."[26]

In short, thinking like the enemy helps you defeat the enemy. Thinking like your competition helps you win against them. Thinking like your boss helps you understand him or her. Thinking like your peers helps you ensure alignment with them.

In the case of cyber espionage, thinking like the adversary doesn't mean you have to act like one. But not thinking like the adversary is cheating yourself from being one step ahead of the enemy. And that is a terrible cybercrime.

The Assumpt! Strategy in Cybersecurity

The goal of the Assumpt! is to raise individual and organizational consciousness in identifying key assumptions and converting them to truth assumptions in order to make faster, smarter decisions. A truth assumption is one that has been surfaced, explored, and tested.

Making an Assumpt! is the act of acknowledging to yourself and others that an assumption is being made while reserving judgment about the specific nature of that Assumpt! Try this. The next time you meet someone for the first time, try to recognize the immediate assumptions you make and turn them into Assumpts! The list is endless but may include, "My Assumpt! is that he or she is successful/is a jerk/has a weak handshake/is a lousy dresser/must be really smart/can't be too bright/isn't very dynamic ..." Then, before acting on that Assumpt!, decide what you want to do with it.

Acknowledging your assumptions opens the door for you to examine your beliefs before acting on them and encourages others to challenge them. This might seem contrary to the directive leadership that kinetic combat often requires, as leaders are expected to "know" to give orders. There are times when this kind of decisiveness is necessary, but at other times, acknowledging your Assumpts! makes for a stronger leader. The following are sample cybersecurity Assumpts! to consider challenging.

> The goal of the Assumpt! is to identify key assumptions and convert them to truth assumptions in order to make faster, smarter decisions.

Case A: A board of directors received a cybersecurity agenda. One of the points was, "Are we doing enough?" This is a common question that many leaders in both the military and non-military ask. But in cybersecurity, *doing enough* assumes the same quantifiable parameters as "Do we have enough insurance?" "Did we budget enough for salaries?" or "Have we spent enough time analyzing the information?" These are good questions, but the assumption is that cyber is finite. It's the difference between looking at the universe that has a beginning and end versus considering the universe as infinite and then reconciling what that means.

Perhaps "Are we doing enough?" could be replaced with "How do we sustain our cybersecurity efforts?" or "What is our strategy for adapting to cybersecurity attacks that constantly change over time?" Acknowledging *enough* as an Assumpt! gives you the ability to shift perspectives and provides new pathways to the solutions you seek.

Case B: The military, like most organizations, believes itself superior to the competition. In cybersecurity, how do you define *superior*? If superiority can be measured by results, then you must assume that you are either winning or losing the war. But in cybersecurity, are you fighting small battles or one big war? If you are willing to see *superiority* as an Assumpt!, then it opens the door that "whatever we do, someone else can do." And rather than assume that is a weakness, see it as a strength because it assures your role on the offense, never underestimating the power of your attacker.

The Assumpt! as an Antidote to Moving Out of Your Comfort Zone

The four steps below outline the Assumpt! flow.

1. **Expand:** Ditch the bias that assumptions are "something I shouldn't make." Accept, without judgment, that assumptions are part of your ladder of thinking and decision-making processes. Within every decision lies an assumption.
2. **Identify:** Listen to the verbal cues generated when moving out of your comfort zone. Be aware of how your present emotional state influences those assumptions. Bring them to the surface. The act of identifying an assumption is called making an Assumpt! Assumpt! is a term coined to help people separate the concept of an assumption from actually making one.
3. **Accept:** Accepting your Assumpts! means acknowledging that you can live with the consequences of where your Assumpt! leads you (i.e., you can leave your Assumpt! "unchecked"). This is an important point as many assumptions are beneficial and serve to help you make decisions quickly and accurately.
4. **Challenge:** This step is when you decide to *check* your Assumpt! My Assumpt! is this is what General Milley was suggesting when he said, "Every assumption we hold, every claim, every assertion, every single one of them must be challenged."[27] There are three levels in the challenge.

   a. **Question:** Questioning this Assumpt! may be as simple as stating, "Perhaps if I tried to do this in a different way ..."

   b. **Explore:** The next level is to explore the Assumpt! in detail to determine the origin of the idea: "What is the Assumpt! based on, and what are the consequences in accepting it?"

   c. **Reject:** The fastest way to create new thinking is to reject your Assumpt! This is what GM did when saying that the production cycle had to adapt to the technology cycle rather than the other way around.

There are more steps to take in identifying and challenging your Assumpts! than outlined in this paper. The main point is that in cybersecurity, we are all learning. And when it comes to moving out of your comfort zone, talent, IQ, and experience don't often matter. Success in conducting business or warfare in unchartered territories is dependent on how you identify and manage the assumptions generated in dealing with the movement away from your comfort zone that drive (in) security.

And it is this author's Assumpt! that this process can change your approach to cybersecurity in as little as one assumption at a time.

NOTES

1. Rick Maze, "Radical Change Is Coming: Gen. Mark A. Milley Not Talking About Just Tinkering Around the Edges," Association of the United States Army, December 13, 2016, https://www.ausa.org/articles/radical-change-coming-gen-mark-milley-not-talking-about-just-tinkering-around-edges.

2. Aron Ralston, interview, *Today*, June 4, 2003 (prerecorded), http://www.nbcuniversalarchives.com/nbcuni/clip/5115075415_s22.do.

3. David McCullough, *The Wright Brothers* (Simon & Schuster, 2015).

4. Thomas J. Shimeld, "Harry Houdini's Final Escape," Chapter 5 in *Walter B. Gibson and The Shadow* (McFarland & Company, 2005), 52.

5. Scott Scheferman, "Ransomware Predictions Past, Present, Future," *ITSP Magazine,* July 7, 2016, https://itspmagazine.com/from-the-newsroom/ransomware-predictions-past-present-future-past.

6. Verizon, *2016 Data Breach Investigations Report* (Verizon, 2016), 6.

7. Jill Anderson, "Remembering Professor Chris Argyris," Harvard Graduate School of Education, November 22, 2013, http://www.gse.harvard.edu/news/13/11/remembering-professor-chris-argyris.

8. Peter M. Senge et al., *The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organization* (Crown Business, 1994), 243.

9. *Department of Defense Dictionary of Military and Associated Terms,* November 8, 2010 (last amended February 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

10. Amazon description of Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy* (Basic Books, 2015), https://www.amazon.com/Red-Team-Succeed-Thinking-Enemy/dp/0465048943.

11. Peter Rus LION, "The Illusion of Being in Control—Part 1," LinkedIn, October 5, 2016, https://www.linkedin.com/pulse/illusion-being-control-part-1-peter-rus; Gerard Koot, "The Water Fortifications of the Dutch Republic," 2014, http://www1.umassd.edu/euro/resources/imagesessays/waterfortificationsofthedutchrepublic.pdf.

12. C. Todd Lopez, "Milley: Army on Cusp of Profound, Fundamental Change," U.S. Army, October 6, 2016, https://www.army.mil/article/176231/milley_army_on_cusp_of_profound_fundamental_change.

13. Ibid.

14. Matthew Cox, "Army Chief Wants Power to Select New Pistol," Military.com, March 10, 2016, http://www.military.com/daily-news/2016/03/10/army-chief-wants-power-to-select-new-pistol.html.

15. Noah Shachtman, "Pentagon's Craziest PowerPoint Slide Revealed," *WIRED,* September 13, 2010, https://www.wired.com/2010/09/revealed-pentagons-craziest-powerpoint-slide-ever/.

16. Andy Cohen, *Follow the Other Hand: A Remarkable Fable That Will Energize Your Business, Profits, and Life* (St. Martin's Press, 2006).

17. Ibid.

18. Ibid.

19. Stefan Cross, "OnStar Tops 1 Billion Customer Interactions," July 29, 2015, http://media.chevrolet.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2015/jul/0729_onstar.html.

20. Much of the information in this section taken from author's personal interviews with Major Jim Twist, October 5 and 25, 2016.

21. *Star Trek II: The Wrath of Khan,* directed by Nicholas Meyer (1982).

22. *Star Trek,* directed by J. J. Abrams (2009).

23. Gregory Conti and James Caroland, "Embracing the Kobayashi Maru: Why You Should Teach Your Students to Cheat," *IEEE Security and Privacy* 9, no. 4 (July/August 2011): 48–51, doi:10.1109/MSP.2011.80.

24. Ibid.

25. Ibid.

26. Ibid.

27. Rick Maze, "Radical Change Is Coming: Gen. Mark A. Milley Not Talking About Just Tinkering Around the Edges," Association of the United States Army, December 13, 2016, https://www.ausa.org/articles/radical-change-coming-gen-mark-milley-not-talking-about-just-tinkering-around-edges.

Growing Role of Platforms in Cybersecurity

Eric G. Troup

ABSTRACT

Platforms are becoming a dominant force in business and software architecture. Regardless of where you look across commercial, government, health or military/defense sectors, platforms are increasingly becoming core features of the digital world. They are at the center of digital ecosystems.

When we think platforms today, it is important to realize that there is a business view, a technology view, and an ecosystem view. Evolving from highly specialized and expensive Service Delivery Platforms, today these multi-tenant and multi-role platforms provide reusable sets of building block capabilities designed to accelerate the growth and to sustain multiple digital ecosystems.

Increasingly today, the technology platform implementation is cloud based and software defined. Furthermore, the cloud infrastructure itself is becoming a commodity. Highly virtualized cloud platforms are dominating because of their huge advantages in automated hyper-scale resource utilization efficiency. The economies of scale are overwhelming.

Platforms enable many important software tasks that would formerly have had to be custom built into each system or application to be accomplished much more effectively by the reusable capabilities provided by the platform. For example, an identity management system provided by a cloud platform can meet the individual needs of hundreds of different services and systems hosted on or accessible via that platform. Thus, by their very nature, platforms are subsuming many of the cybersecurity roles that were formerly performed by individual systems or applications.

The increasing role of platforms requires adjustments to system architecture but, properly approached, offers significant enhancements to cybersecurity. The marketplace recognizes this: *CIO Insight* reported, “52% of (survey) respondents believe cloud apps are as secure, or more secure, than on premise applications, up from 40% last year.” [1]

Eric Troup is Chief Technology Officer for Worldwide Communications and Media Industries, Microsoft Corporation. As the lead industry technology strategist for the Telecom, Cable and Media sectors, Mr. Troup is responsible for influencing the evolution of a growing ecosystem of enterprise solutions for customer and resource management, data analytics, and service orchestration across cloud platforms, software defined networks and devices. He held a variety of leadership positions in the U.S. Army before joining NYNEX in 1985. He held management positions at Unisys and Cap Gemini before coming to Microsoft Consulting Services in 2004.

Mr. Troup earned a Bachelor of Science (BS) degree from West Point, received a Master of Business Administration (MBA) from the University of Utah and is a graduate of the U.S. Army Command and General Staff College. He was the first individual recipient of the NYNEX Chairman's Award and is a TM Forum Distinguished Fellow.

Platforms and the Digital World

In *Platform Revolution,* the authors define a platform as "a business based on enabling value-creating interactions between external producers and consumers." [2] In the continually evolving digital era, platforms are causing some important shifts in focus. We are evolving from monetizing by selling a right-to-use license of a hard-to-make competitive service or capability towards extracting smaller pieces of the recurring value from each of the massive numbers of interactions between producers and consumers in digital ecosystems.

As explained in *Platform Revolution*, the model for valuation of platforms becomes a function of the number of producers and consumers across a network provided the platform itself retains an ability to curate content and moderate network interactions. The focus thus shifts outwardly towards these interactions in a network effect between producers and consumers rather than inwardly on something being produced or licensed by the platform owner. In some cases, items being produced are provided free of charge to not impede growth of the new monetization process. These shifts fundamentally alter the cybersecurity threat surface.

Digital Platform Reference Architecture

Industry groups have been working on standards and best practices for implementing and operating digital platforms and for joining digital ecosystems. The TM Forum [3], in liaison with NIST, ETSI, ITU and Industrial Internet Consortium (IIC) has been evolving its Frameworx [4] to address the needs of digital platforms and digital ecosystems. As part of this effort, the TM Forum is evolving a Digital Platform Reference Architecture (DPRA).

As shown in Figure 1, a Digital Platform has to be understood from both a business and a technology viewpoint. This separation of concerns makes it much easier to understand how to deal with fundamental requirements such as cybersecurity.

DIGITAL PLATFORM REFERENCE ARCHITECTURE

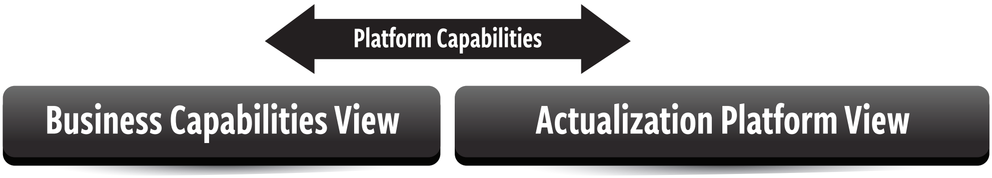


Figure 1. TM Forum Digital Platform Reference Architecture contains a Business Capabilities.

Figure 2 contains an expanded and modified view of the current work-in-progress TM Forum DPRA based upon a recent Microsoft contribution. Microsoft Azure is a commercial example of a platform supporting multiple ecosystems across commercial, public/government, health and defense sectors. The platform provides sets of reusable building block capabilities or services that can be used to create higher-level services. Some of these building blocks can come from the platform maker (First Party services) while others could have been developed by others and exposed via the platform to a community (Third Party services). The Technical Capabilities depicted are an illustrative list and constantly evolving.

DIGITAL PLATFORM REFERENCE ARCHITECTURE

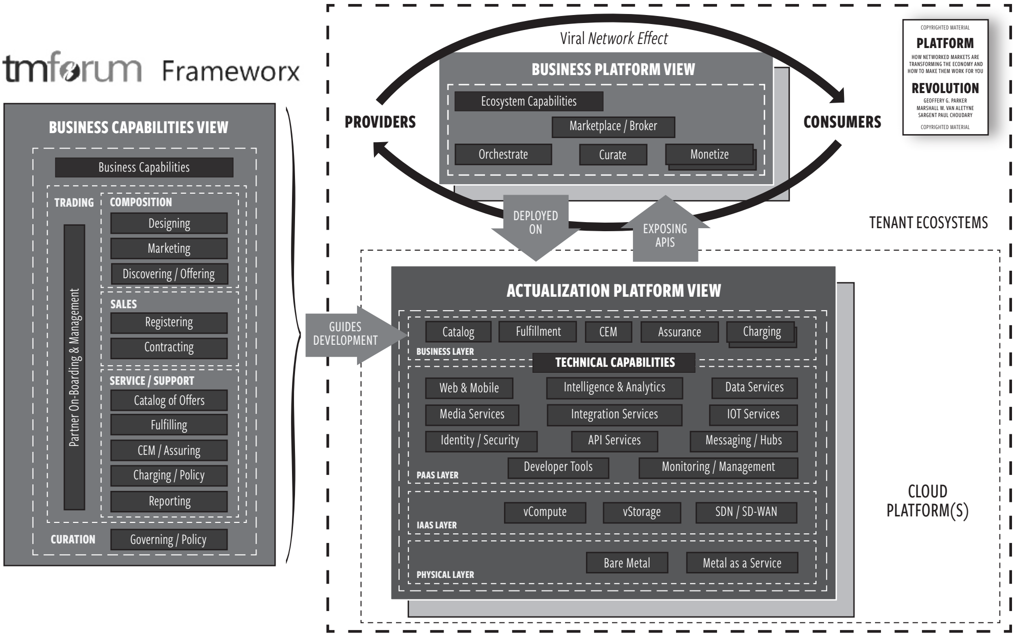


Figure 2. Modified TM Forum Digital Platform with Microsoft Azure adapted Actualization Platform View.

In this context, Uber is a Business Platform with car owners/drivers as providers and travelers being the consumers. It is deployed onto an Actualization Platform.

Microsoft Azure is primarily an Actualization Platform that hosts many Business Platforms; it is multi-tenant yet secure. It is always important to understand which point of view of the platform is being discussed.

The Actualization Platform View makes it easier to visualize the cybersecurity issues across the physical datacenter/network layer, virtualized infrastructure layer, the platform services layer, and business application layer. Each have specific functions to perform as a part of a layered cybersecurity defense.

Distributed Computing / Mobile Edge Computing

Another characteristic of digital platforms is that the services and supporting cloud/network infrastructures are increasingly geographically dispersed. As shown in Figure 3, digital platforms invariable involve chaining together resources hosted across multiple datacenters and devices. Instead of mostly static linear value chains, we have an overlapping value mesh designed to be agile in construction and provide low-latency at the edge. In this context, devices become a part of the platform and thus an integral part of nearly any cybersecurity strategy. Workload placement across the fabric becomes part of the optimization process of highly-automated, close-looped management systems.

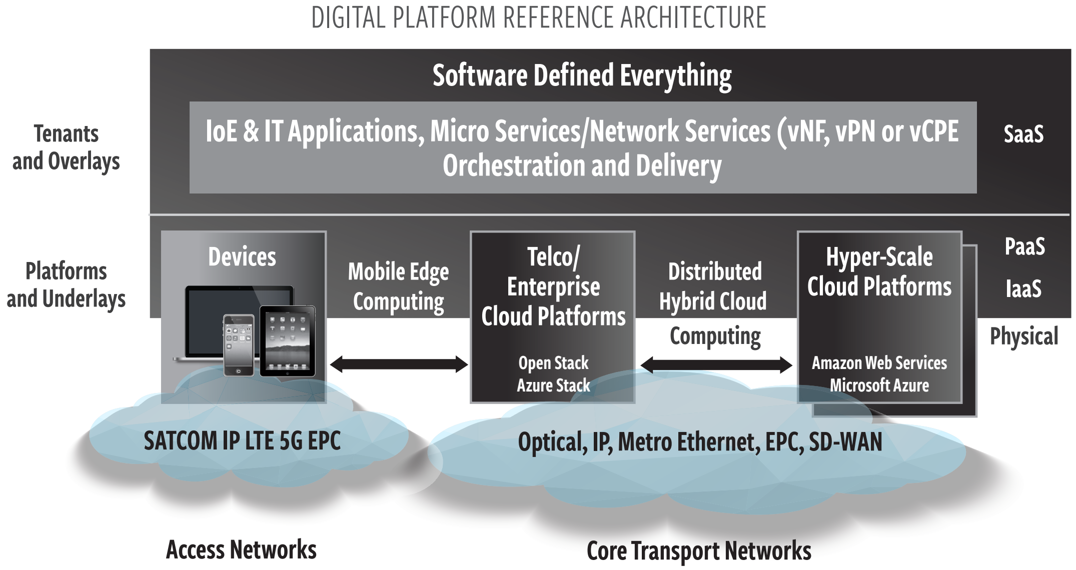

DIGITAL PLATFORM REFERENCE ARCHITECTURE
Software Defined Everything
Tenants and Overlays
IoE & IT Applications, Micro Services/Network Services (vNF, vPN or vCPE Orchestration and Delivery
SaaS
Platforms and Underlays
Devices
Mobile Edge Computing
Telco/ Enterprise Cloud Platforms
Open Stack
Azure Stack
Distributed Hybrid Cloud Computing
Hyper-Scale Cloud Platforms
Amazon Web Services
Microsoft Azure
PaaS
IaaS
Physical
SATCOM IP LTE 5G EPC
Optical, IP, Metro Ethernet, EPC, SD-WAN
Access Networks
Core Transport Networks

Figure 3. Cloud Platforms are geographically distributed for performance and regulatory reasons. This means that platforms must have built-in 'native capabilities' for distributed cloud platform and ecosystem management including cyber-security. They also must be able to gracefully accommodate different security and privacy requirements that may vary by context, country, industry, and tenant.

Platform Workload Types

Digital platforms can also be represented as falling under three fundamental business scenarios for cloud platforms:

1. Internal IT Workloads such as line of business applications, business support systems, operations support systems supporting an organization’s internal requirements.
2. External IT Workloads such as hosting the workloads of external organizations and to implement B2B and/or B2B2C use cases.
3. Internal Network Workloads such as those associated with Network Function Virtualization (NFV), Software Defined Networking (SDN) and Software Defined Wide Area Networking (SD-WAN).

The third category is the newest use case. The telecom and data communications industry is in the midst of a massive $150+ billion worldwide transformation to build a network of cloud based platforms to dynamically host the virtualized network functions that implement and manage the connectivity of people, devices, applications and data leveraging 5G Wireless and IP Evolved Packet Core (EPC) technologies. Eventually all datacenters and networks will not simply employ virtualization but become cloud platforms differentiated only by the nature of the workloads primarily hosted.

> The correct level of cybersecurity will always be a judgment call—but one needs to understand the risks and impacts involved.

As a result, there will be virtually no business scenarios where mission critical data is not flowing across software defined datacenters (clouds) and software defined networks (clouds) invoking allocated resources many of which may not be entirely under the control of any one party.

Having set the stage, let us now look at some cybersecurity principles for digital cloud platforms.

Cybersecurity as a Core Platform Feature

Within the TM Forum, the discussion has begun to shift to Ecosystem Risk Management—addressing the collaborative risks resulting from virtualization and cloudification across an Open Digital Ecosystem. The word “*Open*” here means “*easy to find and consume*”—not vulnerable or free.

While organizations like to believe they have a handle on their own risks—those they own and physically control—increasingly the delivery of a service/product is reliant on a web/ fabric of partners over whom they have less control but have to trust if they are to operate and deliver in this agile new world.

A risk approach was adopted at the TM Forum primarily because members believe there is never a 100% solution to security and any investment in security needs to be appropriate for the value of that being protected. The correct level of cybersecurity will always be a judgement call—but one needs to understand the risks/impacts involved.[5]

On the other hand, for hyper-scale Azure, Microsoft is finding that the costs of providing extensively differentiated levels of cybersecurity is not cost effective and in fact introduces other risks. It is safer to simply provide many of the essential cybersecurity features consistently across the entire Azure ecosystem.

To play in a specific industry environment may require adherence to certain specific security criteria/ standards. When a platform achieves certifications such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS, specific cybersecurity capabilities must be met by that platform.

Security and Privacy Must be Embedded into All Aspects of the Platform

For a cloud platform provider like Microsoft, security and privacy is a priority at every step. For this reason, Microsoft designs its platform and tenant software for security from the ground up. A specific approach known as the Security Development Lifecycle (SDL)[6] is followed. This company-wide, mandatory development process embeds security requirements into the entire software lifecycle, from planning through deployment. To help ensure that operational activities follow the same security priorities, Microsoft has developed rigorous security guidelines laid out in an Operational Security Assurance (OSA)[7] process. When issues arise, a feedback loop helps ensure that future revisions of OSA address them.

> Platforms are increasingly able to provide very robust security protection perimeters but they can never be totally impenetrable.

Security must be able to first protect from and then detect threats. Platforms are increasingly able to provide very robust security protection perimeters but they can never be totally impenetrable. Platforms need to supplement protection with efficient and fast reacting detection mechanisms. Passive and active countermeasures can then mitigate and defeat threats. In some cases, intruders can be sent to honey pots (false data) while then activating cybercrime law enforcement or cyber-warfare counter measures.[8]

Consumer Privacy is another aspect to the cybersecurity regulatory challenge. Over the past year, the TM Forum has focused on privacy as driven primarily by EU legislation (general data protection legislation GDPR) which focuses on giving citizens control over their data and places requirements on organizations collecting data to handle it appropriately (protection, access, etc.). Some of the privacy requirements can be very onerous and their implementation can conflict with certain other certification requirements. Nonetheless, data protection across its lifecycle is critical.

Keeping Customer Data Safe

Hyper-scale cloud-based platforms utilize a robust set of security technologies and best practices including multi-tenant cloud virtualization. These are essential to ensure the cloud platform infrastructure is resilient to attack, safeguards user access to the environment, and helps keep customer data secure. Some specific cyber-security capabilities present on mature, cybersecurity enabled platforms like Microsoft Azure include:

Managing and controlling identity and user access to environments, data, and applications by federating user identities and enabling multi-factor authentication for more secure sign-in. Biometric capabilities on devices such as fingerprints or artificial intelligence enhanced facial recognition enable stronger identity and role-based security.

Encrypting communications and operation processes. For data in transit, use of industry-standard transport protocols between user devices and datacenters and within datacenters themselves. For data at rest, a wide range of encryption capabilities up to AES-256, giving the flexibility to choose the solution that best meets each need.

Securing networks. Infrastructure necessary to isolate tenants and to securely connect virtual machines to one another both with within one datacenter (such as with Clos VL2) [9] and between multiple networked datacenters as in hybrid cloud use cases. Capability to block unauthorized traffic to and within datacenters, using a variety of technologies. Software Defined Virtual Networking to extend on-premises networks to the cloud through site-to-site VPN.

Managing threats. To protect against online threats, offers such as anti-malware for cloud services and virtual machines. Robust intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the platform. [10]

Protecting the privacy of Customers. Time-tested approaches to privacy and data protection including maintaining organizations' ownership of and control over the collection, use, and distribution of their information.

Owning your own data. Customers own customer data—that is, all data, including text, sound, video, or image files and software. Owners should be able to access their customer data at any time and for any reason without assistance. Customer data or derive information from it should not be used for advertising or external data mining without consent.

Trust in the Rule of Law for responses to government and law enforcement requests to access data. When a government wants customer data—including for national security purposes—it must follow the applicable legal processes, in the applicable jurisdiction when serving a court order for content or a subpoena for account information.

Platforms are Strengthening Cybersecurity and Privacy

There are fundamental economic and technical reasons platforms represent such an important force in information technology evolution today. Most people think of the massive network scale required by digital systems today in order to achieve meaningful impact or economic success. To avoid high up-front capital costs, cloud computing platforms are a key enabler to failing fast, adjusting and then achieving successful business growth.

> Platforms, particularly those of hyper-scale, are increasingly in the best position to be able to innovate in cybersecurity.

It takes enormous investment to achieve rigorous adherence to standards for certification or best practices in such mundane areas like cybersecurity. However, cyber breaches represent a very serious and growing threat. As many businesses and government agencies have discovered over the past few years in a series of embarrassing and costly breaches, the threat is very high and growing. The cost of preventing and mitigating has become so significant that most organizations are simply not able to deal effectively with the challenges of a constantly evolving worldwide theat. Having a data center on premise has little to do with securing against cybersecurity threats.

Platforms, particularly those of hyper-scale, are increasingly in the best position to be able to innovate in cybersecurity and maintain on a continuous basis, the necessary large investments. With their huge scale, the larger platforms are much better able to maintain state of art capabilities and invest in costly cybersecurity operations centers equipped with high end, real-time data analytics capabilities and automated artificial intelligence enhanced mitigation capabilities. These costs can be distributed across an increasingly larger customer base.

For essentially the same reasons platforms dominate economically, platforms also enhance cybersecurity. All platform tenants benefit from a much higher level of protection than they could likely secure on their own allowing tenant owners to safely focus more on core businesses. Platforms and the networking of platforms will likely continue to be important to the cybersecurity conversation.

NOTES

1. CIO Insight, http://www.cioinsight.com/it-strategy/cloud-virtualization/slideshows/cloud-apps-rise-despite-cloud-security-concerns.html.

2. Geoffrey Parker, Marshall Alstyne, Sangeet Choudary, *Platform Revolution,* New York: WW Norton, 2016.

3. TM Forum, www.tmforum.org.

4. TM Forum Frameworx https://www.tmforum.org/tm-forum-frameworx – a suite of best practices and standards that provides the blueprint for effective, efficient business operations leveraging proven service-oriented approaches for flexible and agile end-to-end management of services across complex, multi-partner environments.

5. Content in these two paragraphs contributed by Chris Stock, Director Security & Privacy Programs, TM Forum.

6. Microsoft Security Development Lifecycle (SDL); https://www.microsoft.com/en-us/sdl/default.aspx.

7. Microsoft Operational Security Assurance (OSA); https://www.microsoft.com/en-us/SDL/OperationalSecurityAssurance/.

8. Content in this paragraph contributed by Michael Lawrey, Director TM Forum, previously Executive Director at Telstra.

9. Clos network is a kind of multistage circuit switching network, first formalized by Charles Clos in 1952.

10. For additional insights into the level of sustained cyber security investment required see; “Microsoft Announces new Cyber Defense Operations Center, Enterprise Cybersecurity Group; https://blogs.microsoft.com/firehose/2015/11/17/microsoft-announces-new-cyber-defense-operations-center-enterprise-cybersecurity-group/#sm.0001o8vmmz1cold49y-m514udg8bnw and http://blogs.microsoft.com/blog/2015/11/17/enterprise-security-for-our-mobile-first-cloud-first-world/#sm.00000lannxgeojffrx8nvbknohw9x.

The Cyber Defense Review

◆ Research Articles ◆

The Violence of Hacking: State Violence and Cyberspace

Dr. Aaron F. Brantly

The violence of bits and bytes is real. How can we conceive of violence in a digital world? Do traditional definitions provide a reasonable means to understand the impact of violence emanating from cyberspace? This work examines the concept of violence at the state level and builds and argument that violence is not confined to pre-digital static definitions. Like physical violence, cyber violence conducted by states is instrumental and constitutive of both physical and non-physical acts. These acts in combination facilitate state goals, specifically the potential to win wars or achieve related policy objectives. Cyber war is not your father's war, but it has many of the same effects. What are the first, second and third order effects achievable in cyberspace? Are these effects conceptual or have they been demonstrated? What does and can state violence in cyberspace look like and why is it important?

violence *noun* | vi•o•lence : behavior involving physical force intended to hurt, damage, or kill someone or something. [1]

Outside of academia, the definition of violence is broad and far reaching. The word violence typically conjures up very physical and direct notions of the application of force. The World Health Organization defines violence as: "the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either result in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation." [2] The language used to identify violence is straightforward, or so it seems. Over the last several decades and in particular the last ten years a new form of violence has risen to the forefront of global consciousness. Cyber violence can be constitutive of both physical and non-physical, threatened and applied forms of violence. Concepts of cyber violence run headlong into historical semantic debates on the use and value of words extended beyond their core definition.

Dr. Aaron F. Brantly is Assistant Professor of International Relations and Cyber in the Departments of Social Sciences and Electrical Engineering and Computer Science, Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combating Terrorism Center at the United States Military Academy. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights. His most recent book is *The Decision to Attack: Military and Intelligence Cyber Decision-Making* published by the University of Georgia Press.

Many scholars with static semantic approaches to the development of theory claim that cyber violence is not violence as expressed by definition, but something more akin to subversion or manipulation. Semantics aside, violence emanating from cyberspace is a misunderstood concept. Whereas most forms of violence are constitutive of direct or threatened applications of physical force, cyber violence does not often possess a direct causal relationship with the force it creates. Assessing the use of violence by states has long been a core aspect of the study of International Relations (IR). As a field of study international relations privileges the use of concrete language and "good" research methods to identify relationships between phenomena.[3] Within IR even the most hard and fast theories, those rigorously developed and defended over scholarly careers are often under constant and sustained challenges from novel explanations for phenomena.

Rather than being a hard science in which there are laws governing the interaction of phenomena, social sciences largely remain in theory. Scholars test theories over and over, compare them with better explanations for phenomena and then attempt to maintain a hard core of a theory through a positivist heuristic.[4] This paper argues that the definition of violence by states against states is limiting. The present static semantic approach to language within the existing theoretical core focuses on first-order effects of violence to the exclusion of valid and significant second and third order effects not foreseen by original theorists. The semantic rigor associated with the core of many theories obfuscates the reality of most acts of state violence. As the world becomes increasingly digitized and the science fiction of yesterday becomes the science fact of today, it is necessary to incorporate a more encompassing explanation of violence into

IR scholarship. The realization of violence as a complex phenomenon not confined to use or threatened use of physical acts will establish a novel basis for understanding a broad range of legal and policy concepts related to cyber actions as well as more robust models of compellence and deterrence. As the term evolves to encompass actions in new domains of war-fighting, it is necessary to expand the core epistemological foundation upon which we examine novel actions. The semantic understanding of violence is historically relevant, yet its value and importance moving into the future loses utility when explaining new phenomena. Cyberspace is a violent domain. It is violent both in its ability to affect physical violence through first, second and third order effects, but also in its ability violently alter the reality of the world in which we exist in the present. William Gibson wrote of cyberspace as a:

> … consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphical representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters, and constellations of data. Like city lights, receding. [5]

Although the concept of violence in cyberspace is rooted in theoretical foundations and historical semantics, it should not remain static. Despite the semantic and theoretical core, a positive heuristic predicated on modifications to the existing meaning of violence serves to retain the core attributes of the word while expanding its definition to include those acts that are not directly physical. A historically rooted theory based approach is insufficient for an understanding violence in this domain. To understand violence as it pertains to hacking, we must also examine the fundamentals of code, the development of national mission teams and the evolution of society towards a new consensual hallucination, one in which physical and digital violence are linked by the code upon which our lives increasingly depend. The argument below specifically focuses the application of violence through the use of cyberspace as a means to highlight the gaps in present interpretations of law and policy.

Defining Instrumental Violence in War

war *noun* | \ˈwȯr\ : the state of armed conflict between different nations or states or different groups within a nation or state. [7]

States have a history of violence. This violence can manifest in many forms. Yet, violence is by its nature is instrumental. [6] War defined as “the state of armed conflict between different nations or states or different groups within a nation or state” constitutes the application of violence on the largest scale. [7] In focusing on the history of violence by states, I confine this study to the application of violence in the form of war and examine the usage of violence by states for the purpose of achieving political utility. [8] Waltz and other realist theorists contend that war arises out of an absence of an overarching control on a system of anarchy in which states interact.[9] The subsequent use of physical force is intended for the preservation of the survival of the state. As states seek to rigorously establish their security they degrade the security of other states within the system.[10] In its attempts to establish security, the state need not necessarily apply violence, but merely the threat of violence or rather the potential to achieve violence can serve to reduce the security of other states. While realists contend that the focus of this violence is necessarily located in physical security at the top of a needs hierarchy, liberals and in particular, neoliberal institutionalists, contend that the hierarchy of needs is not isolated to the use of physical violence but also to activities that might threaten the survival of a state over time.[11] The threat of violence can and often is a psychological function predicated on the likelihood of survival.

While physical manifestations of force necessarily establish the historical foundations of violence from cavemen to the present. These manifestations have often been paired with the application of threatened force that denies or disarms an enemy through direct action. Thomas Schelling writes: "Forcible offense is taking something, occupying a place, or disarming an enemy or territory, by some direct action that the enemy is unable to block."[12] Violence is the instrumental means by which to achieve an end. While it is likely that Schelling never considered the forcible occupation or disarmament of an enemy or territory absent physical violence, his definition leaves open the use of non-kinetic means to achieve the same ends.[13]

Concepts of cyber violence run headlong into historical semantic debates on the use and value of words extended beyond their core definition.

By constraining the study of violence to the physical world, we ignore the impact of other manifestations of violence that achieve the strategic, tactical and operational objectives that were once only achievable through physical means. While there remains contention on the impact of non-physical violence, there are studies that suggest that alterations in trade and tariff behaviors can increase the likelihood of physical conflict.[14] The denial of assets to a state in the form of a blockade can include either physical or digital forces intended to hurt an opposing state. The siege of Vicksburg is an example of the physical manifestation of the denial of resources to an opposing force.[15] This denial can weaken an opposing force and while a siege or a blockade can be intensely physical and include directed death and destruction from a cannon, muskets, trebuchets and other weapons of war, the forced isolation of group can result in indirect violence through starvation and disease. Economic actions absent physical actions can also result in indirect violence. The closure of markets, the prevention of the sale of goods and services and the disruption of capital flows can hurt an opposing state both physically and psychologically. The generation of second order violence that is not the result of a kinetic action but rather the change in policy or the manipulation of markets is violence and can achieve similar effects.

Violence at its most basic is a physical act. Yet, the application of violence by states need not be physical. There are numerous instances of historical violence perpetrated by states that had less to do with a physical action-reaction causal chain than a linkage between the non-physical instigator of violence (policy, law, code, or position) and a resultant pain, damage, or death of the target. The policies of forced collectivization under Stalin resulted in the losses of millions of lives.[16] The semantic interpretation of the violence of Holodomor would be that of physical violence executed by the soldiers. However, these soldiers were rather a manifest instrument of state violence in the form of policy enforcement. If semantic nuance is to be applied to Holodomor, it would likely absolve the state of culpability in the actions of its soldiers. Based on law and interpretations of responsibility for violent acts, the state retains its authority over those who conduct violence in its name. When a murder occurs police do not absolve the murderer if he used a gun. Despite the disconnect in both physical and temporal space between the action, pulling the trigger, and the effect, a bullet entering and harming a victim, the two parts of the causal chain are linked inexorably.

> The generation of second order violence that is not the result of a kinetic action but rather the change in policy or the manipulation of markets is violence and can achieve similar effects.

The examples above establish that violence is not merely the physical action-reaction relationship it is made out to be. In neither case was the force that injures a person or thing directly physically connected to its origin at the time at which the violence was affected. While the result was indeed a physical result: pain, damage, or death; the instigation of that result can be both physical and non-physical.

Carl von Clausewitz's examination of violence is not confined to physical manifestations as scholars such as Thomas Rid and others have suggested. Rid contends that "Unless physical violence is stressed, war is a hodgepodge notion."[17] Rid goes on to discuss the necessarily instrumental nature of war as defined by Clausewitz. Even Clausewitz notes that violence in war is not tied to the basest of definitions. The instrumentality of violence in the service of an aim is still present.

Clausewitz writes:

> Its violence is not of the kind that explodes in a single discharge but is the effect of forces that do not always develop in exactly the same manner or to the same degree. At times they will expand sufficiently to overcome the resistance of inertia or friction; at others, they are too weak to have any effect. War is a pulsation of violence, variable in strength and therefore variable in the speed with which it explodes and discharges its energy. [18]

pulsation *noun* | pul·sa·tion : [1] the rhythmical throbbing or vibrating or [2] a periodically alternate increase and decrease of quantity (as pressure, volume, or voltage). [19]

Clausewitz locates war as a continuum of violence (i.e. a pulsation). Pulsation defined as [1] the rhythmical throbbing or vibrating or [2] a periodically alternate increase and decrease of quantity (as pressure, volume, or voltage).[19] Total war is not total physical violence, but violence directed to achieve an aim. To achieve this aim pressure is applied differently at different locations. The application of this pressure in the form of violence can often be more effective if it deprives an enemy of their ability to trust the reality in which it exists. The alteration of the calculus of war manipulates the bargaining range of any given conflict and can result in a preferential outcome for the party best able to leverage violence.[20] The bargaining range of states is affected by more than simple brute physical violence. While physical violence can provide a great deal of information, the manipulation or destruction of information streams necessary to assess one's position within the bargaining range can alter a state's perception on what it stands to gain or lose. The manipulation of the information can shift the bargaining range of states.[21] This is not violence in the brutish sense of old but rather violence of the shared information sphere.

Clausewitz again offers support for a more nuanced assessment of violence as a function of war:

> If for the moment we consider the pure concept of war, we should have to say that the political purpose of war had no connection with war itself; for if war is an act of violence meant to force the enemy to do our will its aim would have always and solely to be to overcome the enemy and disarm him. [22]

The object of state violence in the form of war is not aimless, as Clausewitz indicates it is directed towards the achievement of a political objective. This political aim is often the removal of the ability of an adversary to take up arms, while at other times it is the removal of the will of an adversary to fight. In countering Rid's arguments of constraining violence, John Stone writes "the term 'damage' implies that violence may be directed at artifacts as well as people."[23] Stone rightly identifies that violence against artifacts necessarily extends the concept of violence and increases its instrumental value. The elimination of artifacts such as bridges, defense manufacturing centers, and any number of strategic or tactical assets demonstrates the value of applications of violence in pursuit war aims.

Robert Pape notes that when examining strategic bombing there are two major types of coercive air options strategic and interdiction.[24] The first targets military, industry or civilian targets with political or economic value and the second focuses on the lines of supply and logistics. It is here where we see kinetic operations as violence in pursuit of the aims of war. These supply lines, once organized and established via paper and person were susceptible only to kinetic violence. The interdiction of these lines through bombing reduces the effectiveness of military operations. The interdiction of logistical networks in modern warfare is likely to achieve a similar effect.

The dictionary definition of violence is pre-digital. This section illustrated the contradictions and short-sighted applications of the classic dictionary definition of violence in the context of modern warfare. The evidence presented in this section extends the concept of violence from the IR theory outward to its ability to achieve strategic, tactical, operational objectives for political purposes. The remainder of analysis picks up where this one leaves off by examining incidents of non-kinetic violence. The analysis serves to situate cyber violence in a modern, nuanced debate. By establishing the impact of cyber violence, scholars and decision-makers are more likely to thoughtfully examine acts of violence emanating from cyberspace and places them within or extend existing theoretical, legal and policy frameworks.

Establishing The Violence of Hacking

hack *noun* | \'hak\ : use a computer to gain unauthorized access to data in a system.[25]

Our survival in much of the industrialized world is predicated on the systems we have established to manage everything from the mundane all the way up to critical infrastructures that run our electricity, our water systems, financial networks and food distribution. Gibson’s allusion to a consensual hallucination might not be entirely realized, but as a society, we are rapidly advancing down the path towards full integration. The most basic realization of our integration is the absence of fiat currency in our bank accounts. The value of our savings are not stored as dollars or euros in bank vaults but as zeros and ones magnetized onto hard disks. IR literature places a great deal of emphasis on the physical security and the creation of armies, walls, fortifications and other instruments of war that pose both offensive and defensive threats to others, yet there has been substantially less discussion across the discipline on the creation of cyber units by states to undermine the societal structures upon which we depend.

Arguably many of the same activities, to include physical violence can be achieved through first, second and third order effects generated in and through cyberspace. The optimal code execution for violent effect is in and of itself a unique field of study. Below are a series of case examples that serve to highlight the many ways in which code can function in similar ways to conventional kinetic violent acts. The intent is to open the aperture of theorists and policy-makers to the reality of the present and the world to come. Each example is illustrative not of a theoretical possibility but a demonstrated incident in which code affected violence. By understanding how code can affect violence, we are better able to ascertain its strategic, tactical and operational impact in warfare situations. This should provide limited insight into possible uses by adversary states and sub-state actors. It should also highlight the limitations of current theory, law, and policy.

Digital Interdiction of Supply Lines

Our survival in much of the industrialized world is predicated on the systems we have established to manage everything from the mundane all the way up to critical infrastructures that run our electricity, our water systems, financial networks and food distribution. Gibson’s allusion to a consensual hallucination might not be entirely realized, but as a society, we are rapidly advancing down the path towards full integration. The most basic realization of our integration is the absence of fiat currency in our bank accounts. The value of our savings are not stored as dollars or euros in bank vaults but as zeros and ones magnetized onto hard disks. IR literature places a great deal of emphasis on the physical security and the creation of armies, walls, fortifications and other instruments of war that pose both offensive and defensive threats to others, yet there has been substantially less discussion across the discipline on the creation of cyber units by states to undermine the societal structures upon which we depend.

While the scale of violence has shifted in its shock and awe to a point and click the resultant effect is no less severe.

Robert Pape in his article *Bombing to Win* identified different methods of leveraging air power to achieve strategic and tactical objectives. What if the interdiction of supply lines did not require air power at all? What if a state could hack into the supply chain and change orders, destinations of orders, the component attributes of the manufactured supplies and more? Our military is heavily dependent on automated ordering and supply systems distributed across hundreds, if not thousands of contractors and subcontractors, each with a role in facilitating the mission of operational readiness. The introduction of doubt, the reduction in efficiency, the degradation of quality of any given aspect of this supply process could achieve significant impacts. The prospect of an adversary hacking into the US supply and transportation infrastructure for the Department of Defense (DoD) is not speculation, but a present reality.

In April 2013, the Senate Armed Services Committee (SASC) initiated an inquiry into the extent and scope of advanced persistent threat (APT) penetrations into the U.S. Transportation Command (USTRANSCOM). USTRANSCOM's mission is to provide full-spectrum global mobility solutions and related enabling capabilities for supported customers' requirements in peace and war. As one of the nine combatant commands, USTRANSCOM is responsible for managing people trucks, trains, railcars, aircraft, ships, information systems and infrastructure as well as more than 1,203 aircraft and 379 vessels in the Civil Reserve Air Fleet (CRAF) and the Voluntary Intermodal Sealift Agreement (VISA).[26] The Army, The Navy, and the Air Force provide the soldiers, sailors and airmen, but USTRANSCOM gets them to where they need to go and ensures they have the right equipment when they get there. The manipulation of USTRANSCOM in a time of conflict would severely degrade the functional capacity of the US military.

The SASC Report notes that there were at least 20 successful penetrations constitutive of APTs.[27] An APT is a long-term penetration requiring significant and persistent actions by an adversary. While nearly all of these APTs were identified by the FBI, Air Force Office of Special Investigations, the Defense Security Service or the Defense Cyber Crime Center, USTRANSOM was only aware of two.[28] The SASC report notes major failures in information sharing between various government agencies and a fundamental lack of mutual understanding on contractual obligations to share information associated with penetrations into contractor networks.

> Although the effectiveness of STUXNET has received mixed reviews, the ability to damage, disrupt, destroy, and degrade via code is not in doubt.

The penetrations were directly tied to Chinese actors and are in line with China's information operations strategies as outlined in numerous sources.[29] The moves into the transportation and logistics architecture of the DoD has profound ramifications that could undermine the infrastructures established to enable US war-fighting capabilities. The SASC report is careful in its identification of known vulnerabilities and reiterates on multiple occasions "of the at least" indicating that the actual number of penetrations likely exceeded 20. The challenges highlighted by the USTRANSCOM hack are not solely technical, but are illustrative of the challenges faced by multiple overlapping layers of bureaucracies and a strong disincentive on the part of companies to disclose vulnerabilities or exploitations of their platforms for fear of losing position within the lucrative contractor market. The significance of the vulnerabilities highlights that there are violent actions in the form of adversarial actors actively penetrating and seeking to manipulate the critical supply chains necessary for national defense. Objectives once only accomplished by the delivery of tons of munitions are now executed by lines of code with limited risk. While the scale of violence has shifted in its shock and awe to a point and click the resultant effect is no less severe.

The Aurora Experiments and STUXNET Precision Guided Code

Precision-guided munitions are a novelty in the historical lineage of warfare. They serve to hone the lethal focus of an offender onto an objective of importance. This isolation of target facilitates compliance with the Laws of Armed Conflict, in particular, the Geneva Conventions. Precision guided munitions attempt to protect non-combatants from the horrors of war. While mistakes cannot be not entirely avoided they can be minimized and violence can be more appropriately directed against those willingly engaged in conflict.[30] From a conventional arms perspective precision is defined as "The ability to locate and identify a target, strike it accurately in a timely fashion, and determine whether desired effects have been achieved or a restrike is needed."[31]

Markham Schmitt writes:

> Precision lies at the heart of both contemporary air warfare and the law of armed conflict rules that govern it. Precision capabilities increase an attacker's ability to distinguish between military and civilian objectives, thereby fostering compliance with the principle of distinction.[32]

While using precision guided munitions to foster distinction between combatants and non-combatants in the kinetic physical domains of land, sea, air, and space is not without its challenges, the distinction between civilian and military targets in cyberspace is immensely difficult to discern.

While there is no way to fully eliminate the ability of an armored platform like an M1A2 Abrams from firing, the ability to damage its maneuverability or firing efficiency is a real possibility.

The Idaho National Laboratories on March 4, 2007, demonstrated what is now one of the best-documented executions of precision code. Documents declassified by the Department of Homeland Security indicate that the demonstration was initiated after the discovery of a vulnerability known as "Aurora" in the industrial control systems of "spinning machines (generators, compressors, etc.) that are directly coupled to the electric power grid."[33] The test, which cost $2.876 million was designed to highlight vulnerabilities in the nation's critical infrastructure.[34] The test, conducted against a 27-ton diesel generator, demonstrated the impact of targeted code against industrial machinery and resulted in extensive damage and a total loss of generating capability within three minutes.[35] Video of the incident shows the generator violently shaking and billowing black smoke. The code functioned to prevent the safety systems (breakers) of the generator from stepping in. What is most profound about this test is not the test itself in isolation, but the realization that the vulnerability was pervasive across thousands of critical infrastructure nodes.[36]

The demonstration indicated a rapid need for enhanced mitigation of vulnerabilities across the national critical infrastructure and spurred DHS to work jointly with multiple industries through Sector Coordinating Councils. What once would have only been achievable using kinetic weapons leveraging either air power or manned sabotage became a digital reality of cyberspace operations. The ability to affect violence on those systems which run and maintain a society's functional order were found to be susceptible to code manipulations.

The Aurora Generator test was only the first in a series of famous hacks to demonstrate the precision and violence of code. In what is now the most famous cyberattack in history, more so than even the original Morris Worm, is the STUXNET Trojan. STUXNET did not manipulate a single code base but rather multiple interdependent systems each with responsibilities safeguarding the enrichment process of uranium gas into Highly Enriched Uranium (HEU). Although discovered by Sergey Ulasen from VirusBlokAda, the first major write up of STUXNET came from Nicolas Falliere, Liam Murchu and Aric Chien of Symantec.[37]

Whereas the Aurora generator test was conducted in a wholly contained environment under strict conditions, all evidence related to the STUXNET attack pointed towards state involvement.[38] The code leveraged an unprecedented four zero-day exploits in a single weapon system. The code itself was highly targeted and focused its attack against a specific brand of Siemens centrifuges using specific software installations language packs and hardware schematics.[39] The cyber weapon system, STUXNET, is the most complex and integrated hacking incident purported to be conducted by a state actor(s). For this article, what should stand out is its discriminating application of violence. The use of code to damage physical systems and to disrupt their production quality removes the brutishness violence and follows more in line with Sun Tzu than Clausewitz. Whereas a bomb offers its violence in a kinetic reaction, code installs its violence in the underlying logical structure that makes things work. Although the effectiveness of STUXNET has received mixed reviews, the ability to damage, disrupt, destroy, and degrade via code is not in doubt.

Economic Warfare Via Code

There is a plethora of instances in which states in a time of war have attempted to undermine the economic viability of their adversary. During the Revolutionary War, the British recognized the importance of finance for the conduct of war.[40] To undermine the American effort, the British deliberately set about undermining the financial structure of the burgeoning state by counterfeiting the Continental dollar. The concept of the economic manipulation of a state in a time of conflict stems from the assessment that absent the funds to pay and equip a fighting force that force degrades. The Revolutionary War example was remarkably difficult in that it required the forgery and covert distribution of currency into existing markets. The concept was to create rapid influx of fake currency to devalue the Continental dollar. The process of undermining the currency of an adversary in a globally connected world is simultaneously easier to forge and more difficult in to cause a devaluation. While the author knows of no examples of the cyber-enabled devaluation of a currency, there are examples of the theft of currency or the denial of access to currency to achieve strategic and tactical objectives. Moreover, there has been a significant change in how financial transactions are tracked and monitored globally to facilitate state objectives. This tracking and monitoring is a direct result of increased efficiency and connectivity. It is likely these tools, currently demonstrated in isolation against non-state actors, rogue states and targeted individuals within states could extend the effects of economic warfare in ways not yet conceived.[41] Moreover, beyond using the tools of a cybered world to establish constraints on certain actors, criminal organizations, terrorists, and states have demonstrated a willingness to leverage their hacking abilities to raid the financial resources of their perceived targets or adversaries with the intent of augmenting their financial capacity to engage in violence.

There are many examples of state and non-state actors attacking the financial integrity of other states within the international system. Most criminal exploits are undertaken for financial gain. The intent behind state-based attacks is less clear. Attacks by Iran on US banking infrastructure resulting in Department of Justice charges against Iranian nationals are indicative of the early stages of state attacks against financial infrastructures.[42] The North Korean attacks against South Korean financial infrastructure originally known as Dark Seoul, and now referred to as Operation Troy indicate sustained efforts at degrading or damaging financial infrastructure by leveraging multiple attack vectors.[43] These two cases are recent examples of a rapidly increasing number of cases of significant cyberattacks conducted against financial infrastructures in the US and other countries. Although there are active efforts to minimize the risk of cyberattacks against financial institutions through coordination and information sharing through organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The threat landscape is large and daunting and will likely result in the continued convergence of cyber and financial warfare.[44]

Although the use of cyber means to engage in economic warfare is in and of itself not violent in the Clausewitzian sense of war in that death and destruction is not a direct result of the manipulation of financial infrastructures, it does provide an avenue to manipulate the resources the underpin the ability to achieve violence. The analysis within this section is extremely limited, yet the intent is to demonstrate that violence is not independent of the systems which enable it. At the state level, the constraining of resources can degrade the effectiveness of militaries. Cyber means are now far more effective than bombing at disabling, dismantling and constraining the financial resources of state adversaries in most situations.

Hacking Humans

When the writers of *The Six Million Dollar Man* conceived of their show, they likely never considered the ability of states or criminals remotely hacking into to the bionic implants of their star to achieve ulterior goals and objectives. Science fiction is no longer fiction, doctors and patients are actively seeking solutions to a variety of common medical ailments through use of implanted medical devices (IMDs). During the period from 1993 to 2009 approximately 2.9 million US patients received pacemakers.[45] The features of modern pacemakers are extensive, including a variety of statistics and notifications on patient health, sleep modes, alerts for changes in cardiac function and more. Most modern pacemakers have some form of external connectivity that facilitates the collection of data from or programming of the device. Marc Goodman, a former law enforcement officer and author of *Future Crimes*, provides detailed anecdotes about the hacking of limbs, pacemakers, and other devices.[46] Goodman presents a scary future in which criminals hold individuals lives ransom with IMDs or take control of IMDs to achieve other nefarious ends. Like taking control of *The Six Million Dollar Man*, these hypothetical scenarios are chilling and achievable.

> It is incumbent upon scholars and decision-makers to recognize the threats posed by the evolving digital world.

Numerous recent studies from academics as well as the National Institute of Standards and Technology have written detailed analyses of the vulnerabilities embedded within IMDs.[47] One of the most famous IMD hacking incidents occurred when Jerome Radcliffe presented at Black Hat, the world renowned hacker conference. His paper provided definitive evidence that it was possible to hack IMDs. He demonstrated the easy manipulation of various aspects of an insulin pump and provided relevant indications on the effects a hack would have on a human such as himself with an IMD.[48] The result would be death. Although there are no know incidents of hackers engaging in murder extortion through code, the demonstrated capability by Radcliffe and others provides perhaps the clearest direct impact of the manipulation of code for the achievement of violence. The threat posed to IMDs is so great that in a 60 Minutes interview in 2013, Former Vice President Dick Cheney indicated that when he had a pacemaker implanted in 2007, he had doctors disable its wireless capabilities to prevent a potential assassination.[49]

This section builds on other conventional applications of violence that are often more abstract and provides clear, demonstrated capabilities that achieve violence. There is little ambiguity that on an individual basis the ability to kill with code is a reality. While this violence is not universally applicable to entire populations as a bullet or a bomb, it serves to highlight the evolving threat landscape.

70 Ton Paperweights

A 2010 article in the *New York Times* on the number of computers in modern cars brought to the forefront perhaps one of the most effectual ways to accomplish violence through cyber means. The article notes that in 1977, the typical car had one basic computer for spark-plug timing, while today the average consumer vehicle will contain more than thirty computers and more than 100 million lines of code.[50] These computer systems control everything from ignition to breaks and steering and beyond. In 2014 at the Battelle Cyber Auto Challenge a 14-year-old built an electronic remote auto-communications device with $15 worth of Radio Shack parts in a single night.[51] The teen was able to turn on the vehicle and alter some of the non-safety related equipment. Six months later *Wired* columnist Andy Greenberg participated in a test with hackers that illustrated the remote hacking of a Jeep Cherokee while driving down the highway at seventy miles per hour.[52] The controls of the car were hijacked, and the transmission was switched off. The vehicle becomes a rolling paperweight. The hackers in Greenberg's test are not the only ones to demonstrate the vulnerability of cars to digital attacks. There have been multiple papers examining the concept, and even the National Highway Transportation Safety Administration has deemed it of significant concern to publish a 2015 white paper on Vehicle Cybersecurity.[53]

As a best-case scenario, a U.S. Air Force A-10 Thunderbolt II might be able to destroy half-a-dozen or more tanks in a single sortie if it has a near perfect flight. All the while the A-10 pilot must be conscious of threats from multiple other sources to include surface-to-air missiles, anti-aircraft weapons, and other air defense systems. At the same time, a distributed cyberattack against the various control systems that operate an Armored Brigade Combat Team (ABCT) comprised of more than 300 vehicles might be able to immobilize, commandeer the drive components or dramatically reduce the efficiency of onboard targeting computers, forcing soldiers to shift to manual sight. Within the US context as in many other nations, the code bases between the various platforms are similar if not identical. As tanks and other armored components become increasingly imbued with computers such as Russia's T-14 Armata, the potential effect of a cyberattack on one of land warfare's most impressive combat vehicles is astounding. While there is no way to fully eliminate the ability of an armored platform like an M1A2 Abrams from firing, the ability to damage its maneuverability or firing efficiency is a real possibility.

The problem is not confined to terrestrial components of war but extends to naval forces as well. In 2013, a team of researchers at the University of Texas at Austin were able to spoof GPS and divert an $80 million yacht.[54] Cyber vulnerabilities have led the U.S. Navy to reinstate programs focused on celestial navigation.[55] The systems that control the function of naval vessels, particularly on modern ships are increasingly digitized. Peter Singer and August Cole in their novel *Ghost Fleet* highlight the future of warfare in a fictional world where all the modern advances in computing are turned against their operators for military objectives.[56]

Violence in the form of a bomb can pale in comparison to the potential for violence achievable via code. Code, can take a seventy-ton weapon of war and make it into a $6.2 Million fixed artillery battery with manual sights. The reality of the violence of code to affect the tools of war should not be overstated. While there are very real demonstrated incidents of code affecting civilian vehicles and infrastructure, there are no publicly available sources indicating the same kinds of manipulation of associated with military equipment. While not demonstrated, the same underlying computer systems are present in both, and it stands to reason that if one is vulnerable, the other is also.

The Violence of Code

Code is not violent. It is logical representations input into computers. At its most basic code is the on and off of electrical impulses. These impulses direct a computer to engage in an action. Code can be used to create programs that provide insight into the universe, the human body, and efficiencies in transportation, finance, communications, and an almost infinite number of fields. The aggregate benefits of code are immense. Just as a gun can be used for sustenance and target practice it can also be used for killing. Where a gun is limited in its temporal and spatial relations for the achievement of violence, code can extend beyond these limitations and expose assets and individuals to risk in ways that are difficult to comprehend. While the present conceptualization of violence as the physical application of force intended to hurt, damage, or kill someone or something remains in many ways the standard definitional baseline for violence, it is limiting. The above discussion and cases are meant to illustrate that hacking, the unintended manipulation of code when directed towards a violent end can and does achieve violence. The end state of a violent hack has analogs that are well understood and studied by conventional IR theorists, law and policy makers. Just as the increase in weapons quantity and sophistication results in a security dilemma, so to can the development of hacking

The violence of hacking is something that must be addressed and incorporated into existing IR theory, legal and policy frameworks.

capabilities achieve many of the same objectives that a conventional weapon of war might achieve. Likewise, the pervasiveness of code can magnify the impact of non-armed force to include economic and political violence.

It is important not to overstate the threat of violence associated with hacking. The overstatement of the threat diminishes the real risks posed by those who would seek to leverage digital tools for the achievement of violence. At the same time, it is incumbent upon scholars and decision-makers to recognize the threats posed by the evolving digital world. As cars, aircraft, ships, trains, critical infrastructure and even human beings become increasingly digitized the number of potential vectors of violence will increase. Just as black powder increased the lethal range of a projectile, and nuclear weapons increased the destructive radius of conventional bombs, an increasingly pervasive substrate of cyberspace will expand the lethal potential of hacking for violent ends.

The semantic debates of law and international politics are important and help States determine the appropriate normative environment in which they exist. Michael Schmitt outlines a distinction between economic and political coercion and the use of armed force with seven criteria: severity of damage, the immediacy of the consequences, directness, invasiveness, measurability of damage, presumptive legitimacy, and responsibility.[57] These criteria fall outside of codified international law, yet serve as a foundation for future interpretations on the inclusion of non-traditional uses of armed force or state violence such as cyberattacks.

The value of a semantic debate should also not be overlooked. Scholarship by Thomas Rid, Jon Lindsay, Chris Demchak, Martin Libicki, and others serve as a forcing function for civilian and military decision-makers to ensure that the resultant policy frameworks and laws both internal to states and between states are built not on unfounded rhetoric but rather on a conscientious well-defined reality. There is little doubt that as the number of Internet-connected devices expands into the tens-of-billions and these devices seep into every aspect of our lives their ability to generate effects, including those which can result in physical violence will only increase. The violence of hacking is something that must be addressed and incorporated into existing IR theory, legal and policy frameworks. Just as nuclear weapons altered theory, law and policy, cyber weapons stand to do the same.

NOTES

1. “violence.” *Merriam-Webster.com,* 2015, http://www.merriam-webster.com (March 7, 2015).

2. http://www.who.int/violenceprevention/approach/definition/en/.

3. Stephen Van Evera, Guide to Methods for Students of Political Science. Ithaca: Cornell University Press, 1997.

4. Colin Elman, and Miriam Fendius Elman, Progress in International Relations Theory: Appraising the Field. Cambridge: MIT Press, 2003.

5. William Gibson, *Neuromancer* London: Harper Voyager Publishers, 2013.

6. Hannah Arendt, *On Violence,* New York: Harcourt, Brace, Jovanovich, 1970.

7. “war.” *Merriam-Webster.com,* http://www.merriam-webster.com, March 7, 2015.

8. See: Clausewitz, Carl von, Michael Howard, and Peter Paret, *On War,* Princeton, NJ: Princeton University Press, 1976, 43.

9. Kenneth N. Waltz, *Theory of International Politics.* Reading, Mass: Addison-Wesley Pub. Co 1979 102-104.

10. Robert Jervis, “Cooperation Under the Security Dilemma.” *World Politics* 30 (2), Cambridge University Press, Trustees of Princeton University, 1978, 167–214.

11. Robert O. Keohane, and Joseph S Nye, Power and Interdependence: World Politics in Transition, Boston: Little, Brown, 1977.

12. Thomas C. Schelling, Harvard University, Center for International Affairs, 1966. *Arms and Influence.* New Haven: Yale University Press, 79.

13. Specifically here the intent is to indicate that the connection between the objective and the instrumental act of violence necessary to achieve that objective can and often does originate within a first order effect. However, violence is not constrained to first order effects.

14. Solomon W. Polachek, John Robst, and Yuan-Ching Chang, “Liberalism and Interdependence: Extending the Trade-Conflict Model,” *Journal of Peace Research* 36 (4), SAGE Publications: 1999, 405–22.

15. A. A. Hoehling, and Army Times Publishing Company, *Vicksburg: 47 Days of Siege,* Englewood Cliffs, NJ, Prentice-Hall, 1969.

16. Serhii Plokhy, “Mapping the Great Famine,” *Gis.Huri.Harvard.Edu.* Accessed February 28, 2016. http://gis.huri.harvard.edu/images/pdf/MappingGreatUkrainianFamine.pdf.

17. Thomas Rid, “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35 (November 2012): 7.

18. Carl von Clausewitz, Michael Howard, and Peter Paret, editors, *On War,* Princeton:Princeton University Press, 1976, 87.

19. “puslation.” *Merriam-Webster.com,* http://www.merriam-webster.com,March 7, 2015.

20. See: JD Fearon, “Rationalist Explanations for War.” *International Organization* 49 (3): 1995, 379–414.

21. Aaron F. Brantly, “Cyber Actions by State Actors: Motivation and Utility.” *International Journal of Intelligence and CounterIntelligence* 27 (3): 2014, 465–84.

22. Carl von Clausewitz, Carl von, Michael Howard and Peter Paret editors, *On War,* Princeton: Princeton University Press, 1976, 87.

23. J. Stone, “Cyber War Will Take Place!.” Journal of Strategic Studies 36 (1): 2013, 101–8.

24. Robert Anthony Pape, Bombing to Win: Air Power and Coercion in War. Ithaca: Cornell University Press, 1968.

25. “hack.” *Merriam-Webster.com.* 2015. http://www.merriam-webster.com (March 7, 2015)

26. http://www.ustranscom.mil/cmd/aboutustc.cfm

27. Senate Armed Services Committee, Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors, United States Senate, 113th Congress, S. REP. NO. 113-258, at (2014).

28. Ibid.

29. Jon R. Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39 (3): 2015, 7–47; Kramer, Franklin D, Stuart H Starr, and Larry K Wentz, 2009 “Cyberpower and National Security.” Washington, D C; National Defense University Press: Center for Technology and National Security Policy; Potomac Books, William T. Hagestad, *1st Century Chinese Cyberwarfare.* Cambridgeshire [England]: IT Governance Pub, 2012.

30. International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention),* August 12, 1949, 75 UNTS 287, available at: http://www.refworld.org/docid/3ae6b36d2.html [accessed May 31, 2016].

NOTES

31. Michael N. Schmitt, Precision Attack and International Humanitarian Law, 87 INTERNATIONAL REVIEW OF THE RED CROSS, 2005 445, 446.

32. "Precision Air Warfare and the Law of Armed Conflict." *International Law Studies* 89: 2013, 694.

33. 14f00304 Documents https://d3gn0r3afghep.cloudfront.net/foia_files/14f00304-Documents.pdf from https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#1212530-14f00304-documents, see 36.

34. Ibid., 57.

35. Ibid.,59-62

36. Ibid., 70-72.

37. Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier ." Version 1.4 Symantec, 2011.

38. Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York: Crown Publishers, 2014.

39. Ibid.

40. Ben Baack, "Forging a Nation State: the Continental Congress and the Financing of the War of American Independence", *Economic History Review* 54 (4). Wiley-Blackwell: 2001, 639–56.

41. Exec. Order No. 13660, 31 C.F.R.(2014).; Juan Carlos Zarate, Juan Carlos, Treasury's War : the Unleashing of a New Era of Financial Warfare. New York: Public Affairs, 2013.

42. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities | USAO-SDNY | Department of Justice." *Justice.Gov,* 2016, Accessed June 7. https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

43. Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea." McAfee, 2013, http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf.

44. Juan C. Zarate, "The Cyber Financial Wars on the Horizon." Foundation for the Defense of Democracies, 2015. http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf.

45. Arnold J. Greenspon, Jasmine Patel, Edmund Lau, Jorge A. Ochoa, Daniel R. Daniel R. Frisch, Reginald T. Ho, Behzad B. Pavri, and Steven M. Kurtz, "Trends in permanent pacemaker implantation in the United States from 1993 to 2009: increasing complexity of patients and procedures," Cardiology Faculty Papers, 2012, Paper 18.

46. Marc Goodman, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, New York: Doubleday, 2015.

47. Division, NIST Computer Security, and Electrosoft Services, Dr Sarbari Gupta, *Implantable Medical Devices - Cyber Risks and Mitigation Approaches,* 2012. http://csrc.nist.gov/news_events/cps-workshop/cps-workshop_abstract-1_gupta.pdf; Halperin, Daniel, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H Maisel, "Security and Privacy for Implantable Medical Devices." *Pervasive Computing,* January, 2008, 30–39; Tamara Denning, Alan Borning, Batya Friedman, Brian T Gill, Tadayoshi Kohno, and William H Maisel, "Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices," 2010,917–26.

48. Jerome Radcliffe, Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, 2011, https://media.blackhat.com/bh-us-11/Radcliffe/ BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

49. http://www.cbsnews.com/news/dick-cheneys-heart/.

50. Jim Motavalli, "The Electronic Systems That Make Modern Cars Go (and Stop)." *The New York Times,* February 4, 2010.

51. Lucas Mearian, "With $15 in Radio Shack Parts, 14-Year-Old Hacks a Car." *Computer World.* February 20, 2015, http://www.computerworld.com/article/2886830/with-15-in-radio-shack-parts-14-year-old-hacks-a-car.html.

52. Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It." *Wired.com.* July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

53. Stephen Checkoway, Damon McCoy, Brian Kantor, David Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, and Franziska Roesner, "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In, 1–16.; 2015. NHTSA and Vehicle Cybersecurity | National Highway Traffic Safety Administration (NHTSA). Nhtsa.Gov, 2011.

NOTES

[54] Erik Zumwalt, "Spoofing a Superyacht at Sea." *News.Utexas.Edu.* July 30, 2013. http://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.

[55] "U.S. Navy Brings Back Navigation by the Stars for Officers." *NPR.org.* Accessed June 7, 2016, http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers.

[56] P.W. Singer and August Cole, *Ghost Fleet: a Novel of the Next World War.* Boston: Houghton Mifflin Harcourt, 2015.

[57] Michael N. Schmitt, "The 'Use of Force' in Cyberspace: a Reply to Dr Ziolkowski," 2012, 1–7.

Encounter Battle: Engaging ISIL in Cyberspace

Dr. Chris Bronk
Gregory S. Anderson

INTRODUCTION

Although the United States withdrew its last remaining combat forces from Iraq in December 2011, a significant insurgency spanning the territory of Iraq and Syria has evolved under a variety of names including the Islamic State, Islamic State in Syria (ISIS) and the Islamic State in Iraq and the Levant (ISIL)—for this work, we choose to employ the title ISIL. Since ISIL's break with al-Qaeda in February 2014, it has become the chief standard-bearer of a Salafi jihadist movement set upon forming a trans-regional caliphate. In its activities, ISIL has extended its territorial reach across North Africa and the Arabian Peninsula as well as claiming credit for terror attacks from Belgium to Bangladesh. As much as a movement, ISIL is the contemporary brand for Jihadist insurgency in the Middle East and beyond.

While ISIL forces have made impressive territorial gains in Iraq and maintained a viable resistance to Syria's Assad government, it is now extending its reach into the digital domain, cyberspace, to further its ambitions in intelligence collection, propaganda, and recruitment. Also, ISIL is perhaps the first violent insurgent or terror group to seriously consider developing at least modest cyberattack capabilities as well as developing strength in sophisticated computing and communications technologies designed to defend the identity of its adherents and the security of their digitally-mediated interactions. [1]

For the US, the fight against ISIL also represents a significant test of its offensive cyber capabilities. Yes, ISIL has put US allies on the defensive, but if U.S. Cyber Command (USCYBERCOM) is to be a viable part of the Department of Defense's (DoD) mix of forces going forward, it will need to demonstrate how it can be of utility in the counter-insurgency and counter-terrorism struggle against ISIL and its confederates. The fight against ISIL will represent a significant test of USCYBERCOM's ability to

Dr. Chris Bronk is an Assistant Professor of computer and information systems at the University of Houston's College of Technology. He holds or has previously held appointments in Rice University's computer science department and Baker Institute for Public Policy and at the University of Toronto's Munk School of Global Affairs. Until 2006, he served as a career diplomat with the U.S. Department of State on assignments both overseas and in Washington, D.C. He recently published the book, *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security.*

operationalize tactical capabilities in line with strategic goals of marginalizing and eventually defeating this organization.

Provided here are observations of ISIL cyber power, from digital information operations and intelligence, to operational security and desired future capabilities. We also examine open-source material and reporting on US cyber operations against ISIL and leadership statements from the DoD and others in US government. Finally, we offer a prescriptive component that connects desired outcomes for diplomatic activities and military operations aimed against ISIL in the U.S. Central Command (CENTCOM) area of responsibility (AOR)—20 nations in the Middle East, Central and South Asia with cyber options, both known and desired.

Contemporary Counter Insurgency Operations in the Middle East

Although ISIL's roots are with the al-Qaeda terror organization in Iraq, it has embarked upon a far more ambitious agenda for Islamic statehood that combines previous operational tradecraft in terror operations with a clear desire to capture and hold significant territory and generate economic activity sufficient to challenge state authority in its primary operating theater—Iraq and Syria. Combat operations against ISIL by outside military forces, including those of Iran, the US (along with Coalition allies), and Russia began in the summer of 2014. Russia deployed air and ground forces to Syria; however, fighting ISIL has created a coalition of rather unusual bedfellows.

Iran, a US adversary since the 1979 Revolution, has a significant stake in supporting the Iraqi coalition government, with its large Shia representation.[2] To this end, Iran has provided both military advisers to the Iraqi army and pro-government Shia militias. In parallel with the

Gregory Anderson is a master's candidate for the Information Systems Security program at the University of Houston and is currently a research assistant under Dr. Chris Bronk and Dr. Arthur Conklin. He earned his bachelor's degree in Business Computer Information Systems from the University of North Texas.

Iranian intervention, the US has gradually reintroduced forces into Iraq, a number that stands at 4,650 as of July 2016. In addition to advisers and logistical support, the US maintains significant numbers of manned and unmanned aircraft in the region that have been employed in intelligence, surveillance and reconnaissance (ISR) missions as well as air strikes against ISIL forces. Russia's involvement appears confined to Syria, in the form of air power and limited numbers of ground forces. Russia has also aided autonomous Kurdish forces in Syria.[3]

The Kurdish dimension to the ISIL conflict in Iraq and Syria further broadens the set of interested parties, most significant among them Turkey. Considerable US and coalition resources have gone into supporting Kurdish military forces in Iraq. While the Iraqi Army collapsed in the face of the 2014 ISIL offensive, Kurdish troops have been viewed as more effective in protecting territories viewed as their own, but they are not without internal issues.[4] Also, Iraq's current president, Fuad Masum, is an ethnic Kurd. While the interplay of Iraqi internal politics is of limited salience here, the Kurdish issue and the threat to Turkey produces interesting cyber geopolitics relevant to the conflict as the Erdogan government has routinely found issue with the actions of its internal opponents on social media.[5]

Military operations against ISIL undertaken by the US-led coalition cohere well with the form of conflict summarized by now retired Admiral James Stavridis, the former NATO commander. His view of contemporary and future conflict is that it will be dominated by drones, special operations forces (SOF), and cyber.[6] This is the force mix that the US and its allies have fielded in Iraq and, to a lesser degree, Syria. Besides the US, Australia, Canada, Denmark, Germany New Zealand, Norway, Spain, and the United Kingdom have deployed ground contingents, primarily composed of military advisers in Iraq and Iraqi Kurdistan along with an air component. Many of the SOF are called upon for direct action operations aimed to rescue hostages, identify targets for precision munitions, or neutralize ISIL leadership targets.

The other highly visible activity in counter ISIL operations is air power. The Russian and Coalition air forces have used precision air strikes and drone attacks to counter ISIL. Among the US-led coalition conducting air strikes has been Arab nations Jordan, Morocco (withdrew 2015), and the United Arab Emirates. Michal Eisenstadt stresses that “The campaign against ISIS cannot be won by airpower alone.”[7] While it can be and likely has been useful in breaking up large concentrations of ISIL ground forces, it is less so as ISIL goes to ground. As former MI6 officer and EU adviser Alastair Crooke observed, air strikes, “‘are more likely to kill people who are not involved because the practice of these groups is to break up their formations, dissipate and then move on to built-up areas and hide within the populations.’”[8]

There are concerns for spillover of the conflict into neighboring countries, including Turkey, Saudi Arabia, and Jordan. With a lengthy land border with Iraq and Syria as well as its concerns regarding its Kurdish minority, Turkey has much to fear regarding Islamic terrorism on its soil as well as strong Kurdish forces in the region. Less a factor in counter-ISIL operations has been Saudi Arabia, which has trained token numbers of fighters for operations in Syria. However, the Kingdom has been a target of violence by ISIL confederates in recent months, including the holy city of Medina.[9] Finally, Jordan, which hosts more than a million Syrian refugees, is already stretched thin in extending its national resources to provide humanitarian support.

ISIL is perhaps the first violent insurgent or terror group to seriously consider developing at least modest cyberattack capabilities

Why They Fight—ISIL Social Media & Propaganda

Use of social media to distribute Jihadist messages arose almost as quickly as the technology was invented. In the hands of Jihadist groups, it is an outgrowth of a socially mediated network in which video and audiotape messages are copied and recopied then passed across the Middle East and beyond. Popular are videotapes of hostages (usually Western) employed to demonstrate strength and opposition to the West. These videos were previously used to demonstrate proof of life, after 9/11, Abu Musab al-Zarqawi and other al-Qaeda leaders released execution videos of hostages. The brutal videos are now a staple of ISIL propaganda.[10] Their stature rose significantly in 2014 when ISIL officially parted ways with al-Qaeda and released the beheading video of American journalist James Foley. ISIL pushes its media through online sites as well as major American platforms, including YouTube and Twitter.

To understand the ISIL narrative, it is important to grasp the medium it attempts to master. ISIL has maintained a heavy presence on social media platforms including Twitter, [11] Instagram, and YouTube to maximize exposure for their propaganda related activities. While the Twitter platform is not built for sustained diatribes, their brief 140 character updates allow for a constant flow of reinforcement. Instagram represents another vehicle for propaganda distribution available to ISIL and a useful image-based complement to Twitter. Instagram's primary function is sharing videos and pictures. The proliferation of high-quality cell phone cameras and Go-Pro type lightweight mobile cameras, allows ISIL to share, in morbid detail, their most violent exploits with just a few clicks. [12] These activities plainly violate the terms of service of these sites, and both Twitter and Instagram have taken steps to stop the spread of ISIL propaganda, including, but not limited to, blocking known ISIL accounts. [13]

The fight against ISIL will represent a significant test of the ability of USCYBERCOM to operationalize tactical capabilities with strategic goals of marginalizing and eventually defeating this organization.

The Internet provides ISIL unique reach across the world to "become pen pals with a lonely teenager in small-town America." [14] Not only are their social media attempts to recruit fence-sitters and sympathizers to travel to the Middle East or carry out terror attacks in their home country; they are forcing the West to send troops to combat ISIL on the ground. By provoking a US and coalition military response, ISIL plays the victim and reinforces their claim that "the West is engaged in a crusade against Muslims." [15]

ISIL has successfully made full use of so-called 'viral' marketing campaigns to establish itself on the Internet. ISIL has created its own brand, networked with other terrorist groups, and engaged with their supporters through social media. [16] Through their media campaign, ISIL recruits from around the world, including Usaamah Rahim of Boston, Massachusetts, who sought to kill police officers. [17] Rahim was radicalized via internet correspondence and expressed sympathies for ISIL on social media. [18] As with al-Qaeda, ISIL has a well-staked interest in radicalizing persons already living in the US and other Western countries to engage in terror attacks. These individuals, exemplified by San Bernardino terrorist shooters Rizwan Farook and Tashfeen Malik, often operate alone or in small tightly knit groups, represent the most paradigmatic ISIL assets to strike targets beyond the Middle East. ISIL also calls for adherents to travel to the Middle East for training and participation in military action in Iraq, Syria, or other operational areas. [19]

As of August 2014, "as many as 3,000 Westerners" were recruited and fighting alongside ISIL and related jihadist groups in Syria and Iraq. [20] ISIL constructed a sophisticated online media machine masterfully crafted for recruiting Westerners. One such media activity is the Al Hayat Media Center, established in May of 2014, and publishes in French, German, and English. Most of the posted content is in English, which strongly "suggests that they are specifically designed as a recruitment tool for Western audiences." [21] One of the programs run by Al-Hayat is called mujatweets (mt), which showcases the group's domestic efforts of winning support by showing the "lighter side of life in ISIS." One example is called "Cats of Jihad," in which ISIL fighters pose cats with their weapons. [22]

The U.S. Department of State has estimated that roughly 12,000 foreigners from 50 different countries have traveled to Syria to fight with ISIL, with most between the ages 15 and 25. [23] It is alleged that one-third of the 12,000 foreign ISIL fighters are from Western countries. [24] ISIL tends to focus their recruiting efforts on Western youth (evident by the high amount of English propaganda). ISIL recruiters discern if the potential fighters are more likely to join ISIL in the Middle East or carry out terrorist attacks in their home country. ISIL recruiters create an online community encouraging recruits to break ties with any outside channel that could disrupt the recruitment process (e.g. family and friends). [25] Many ISIL recruits become cannon fodder and are encouraged to further the brutal propaganda campaign by creating videos and "blowing themselves up." [26]

> Contemporary and future conflict will be dominated by drones, special operations forces (SOF), and cyber.

The recruits that do not head to Syria or Iraq are strongly encouraged through the online ISIL community to carry out terrorist attacks in their home country. As the organization has said of the West, "the tiniest action you do in the heart of their land is dearer to us than the biggest action by us. There are no innocents in the heart of the lands of the crusaders." [27] Online recruiters offer guidance on how to carry out an attack and offer resources on how to construct or acquire materials if necessary. ISIL considers Western Lone Wolves a relatively cheap resource for ISIL. If a Lone Wolf carries out a terrorist attack, ISIL can choose to claim credit or not, depending on its outcome. Lone Wolves are also incredibly useful as they typically use their financial resources to carry out attacks.

ISIL's Cyber Capabilities and Intent

While the Internet has served as an important vehicle for recruiting adherents to Jihadist causes, the US and its allies must prepare for ISIL's expanding capabilities. Recruitment is but one measure of ISIL's power. There are many others, including its financial resources, the capacity to communicate at a distance, ability to plan and execute coordinated operations, and acquire increasingly sophisticated armaments and use them effectively in traditional and unconventional combat operations.

ISIL has also made liberal use of Facebook Groups to conduct arms trafficking, including the sale and transfer of small arms and other munitions.[28] These Facebook Groups closely mimic American legal counterparts with the open posting of ads with pictures, descriptions, and prices for everyone to see. However, Facebook's terms and policies updated in January 2016 have disallowed all open trading of firearms and other munitions for all users regardless of country or affiliation.[29] Unfortunately, Facebook relies heavily on the user to report violations of these terms.

ISIL and other groups aligned with it have also started moving secure activities to other social media websites such as Diaspora.[30] Diaspora is a decentralized social network with data stored on private servers (called pods) not controlled by Diaspora's staff. This leaves the removal of ISIL (and ISIL-related) content up to the owner of the pod. These additional platforms do not allow for the widespread dispersal of propaganda of Twitter and Instagram, however, it does let them operate with more impunity. Also, ISIL appears to have a growing awareness of digital operational security. Although many of the group's operations have employed open, unencrypted communications, researchers from the Combating Terrorism Center (CTC) at West Point located a 34-page operational security manual originally drafted by a Kuwaiti firm as advice to journalists and activists in Gaza, which ISIL now uses as an essential training tool.[31]

ISIL maintains a heavy presence on social media including Twitter, Instagram, and YouTube to maximize exposure for their propaganda related activities.

Despite social media sites attempts at preventing the spread of ISIL imagery, news, and other content, they are operating within the watchful eye of the world in most forms of commonly accessed social media. America's long history of trying to 'win the hearts and minds' of civilians in counterinsurgency operations stretches back as far as the Philippine-American War (1899-1902). ISIL recognizes the ideological struggle with the US and employs the Internet as its most valuable outlet for promoting public narratives useful to the organization. With regard to combat operations, this places US and Coalition forces in a precarious position, just as insurgencies can wreak havoc to an organized force with strictly enforced rules of engag ment, the fight against ISIL adds the additional concern of a global audience witnessing any misstep resulting in collateral damage and civilian fatalities. Finally, ISIL overarching information operations intimidated 1,700 Iraqi forces into surrender when some 1,500 ISIL fighters took control of Mosul from some 30,000 Iraqi soldiers and police in June 2014. ISIL's effective use of social media has brought further support to their cause.[32]

ISIL has so far proven itself very adaptable to the changing terror environment by seeking new ways to impose its jihad on the West. For now, these attacks have largely remained rudimentary in nature. In a few cases, they have gained access to Twitter feeds of US military members involved in CENTCOM operations or defaced websites of US military spouses.[33] These attacks have failed to influence military operations, but represent early steps in the development of an offensive cyber platform. Furthermore, ISIL is openly talking online about hacking aviation instruments of large passenger aircraft as well attacking nuclear power plants to release deadly radiation.[34] While these attacks have yet to materialize, ISIL is in the early stages of intrusion into the US power grid.[35] These attacks have been entirely unsuccessful and low level, however, it paints a clear picture of ISIL intent. These intrusions were executed with basic attack software purchased through online Dark Net market websites such as the Silk Road and its successors. By using social media, ISIL seeks to internally produce malware for future attacks while also accessing code manufactured by hackers for hire.

Through social media ISIL seeks to internally produce malware for future attacks while also accessing code manufactured by hackers for hire.

Additionally, ISIL will make better use of bot software to spread their message through Twitter. Currently, the traditional system of making thousands of accounts to swarm feeds and hashtags, both items that increase message visibility, is being countered by Twitter.[36] However, new apps (such as the Android app *The Dawn of Glad Tidings*) are now built allowing predetermined messages by ISIL social media coordinators to slowly spread through users with real accounts who choose to opt in.[37] When a user opts-in, their account functions 'normally', but will periodically broadcast ISIL tweets that are also sent around at the same time to thousands of other accounts.[38] These accounts are difficult to detect and allow for users who already have large amounts of followers to get their message out.

Usage of the app even varies the timing of posts to minimize detection and to maximize exposure during offenses. During the Mosul offensive, the ISIL controlled accounts sent out over 40,000 tweets.[39] ISIL has recognized the new threat network that advanced attacks on US systems can provide through cyber warfare, and the US must counter this adversary.

The ISIL Cyber Complex

ISIL can and will conduct cyber warfare operations, which poses a significant threat to US interests and security. Through cyber operations, ISIL's sphere of influence extends beyond Iraq and Syria. While capabilities do not yet meet ambitions, ISIL is focused on conducting cyberattacks against critical infrastructure targets, including the US electrical grid.[40] Unlike cyberattacks from China, Iran, and Russia; ISIL hackers are more devoted to their cause and will overtly engage in hostilities against the US and its allies. ISIL cyber capabilities are not on par with nation-state actors, but their determination is found in the exploits of two ISIL-aligned computer hackers: Junaid Hussain and Ardit Ferizi. Neither Hussain's nor Ferizi's origins are in Syria or Iraq, but rather Europe.

Junaid Hussain rose to prominence in Jihadist hacking circles in 2011 when he compromised the digital address book and personal accounts of former UK Prime Minister Tony Blair. Using the hacker handle, TriCk, Hussain was just 17 years old when British authorities jailed him. Hussain, a British-born hacktivist turned pro-ISIL hacker of Pakistani descent became involved with the TeaMp0isoN Islamic hacking organization, contributing to the group's efforts. Other members of his hacking group, TeaMp0isoN, reputedly overloaded MI6's counter-terror hotline later that year. He was politicized through violent videos against children in Palestine and Kashmir, Hussain told an interviewer of his motivations in 2012:

As hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends

> I wanted to know why this was happening and who was doing it; there were loads of questions in my head. It made me angry; it changed the way I lived my life and the way I saw the world. I then started using hacking as my form of medium by defacing sites to raise awareness of issues around the world and to 'bully' corrupt organizations and embarrass them via leaks etc., which is how I got into hacktivism.[41]

Upon release, Hussain made his way to Syria with his British wife, a convert to Islam, and set to work training the ISIL organization in cyber tradecraft. He was an associate of Mohammed "Jihadi John" Emwazi, the ISIL spokesperson known for his role in killing Western hostages James Foley and Steven Sotloff. Hussain achieved results hacking CENTCOM Twitter and YouTube accounts.[42] More threatening was Hussain's employment of a technique known as 'doxing' to build dossiers of personally identifiable information found online regarding Coalition service members and their families.[43] The capacity for

ISIL digital operatives to pass such information along to confederates in the US or Western Europe willing to attack relatively soft targets is a serious concern.

For some time, scholars of the law of armed conflict have considered the question of when a nation-state would meet a cyberattack with a kinetic response. The killing of Junaid Hussain on August 24, 2015, during a US airstrike in Syria appears to have answered that question.[44] In killing Junaid Hussain, the Pentagon displayed a capacity to meet cyber power with kinetic force. It appears that Hussain is the first terrorist hacker to be explicitly targeted by the US in a military campaign—the 2011 killing of Anwar al-Awlaki in Yemen via a September 2011 drone strike offers an example of prior military action to disrupt terrorist recruiting via the Internet.

Beyond the Hussain strike, the US has initiated a 'doxing' prosecution of Ardit Ferizi, a Kosovar studying computer science in Malaysia. He was arrested in October 2015, after allegedly breaching a retailer's database and lifting records of all its military and government customers. US prosecutors allege, "Ardit Ferizi is a terrorist hacker who provided material support to ISIL by stealing the personally identifiable information of U.S. service members and federal employees and providing it to ISIL for use against those employees," and provided Hussain with this information between June and August 2015.[45]

Since Hussain's death, ISIL has continued to mount cyber campaigns, but its aspirations appear far greater than its capabilities.[46] Yes, ISIL can hire individuals online to act on the group's behalf in launching cyberattacks, but likely only to a limited degree.[47] ISIL cyber operatives continue to develop their technological skills as they shield their communications from eavesdropping, utilize encrypted chat systems and employ fake phone numbers. Although, cyberattacks are low threat and can be stopped, ISIL is beginning to learn and hone their skills.[48] As hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends. Soon the US will face a major cyber capability in the hands of a Jihadist group or groups.

> Translating desired policies into a real, viable cyber campaign is the unique challenge of the moment.

Policy Options—Cyber Offense Against ISIL

Although ISIL's military capabilities in Iraq and Syria have been significantly blunted, the organization remains a potent force. The challenge in further reducing ISIL's cyber capabilities is two-fold. The US and its allies must work to harden military, critical infrastructure, and economic targets. Mitigating the ISIL social media machine is a difficult but necessary task. There is no silver bullet available to resolve the power of pro-ISIL narratives particularly since Muslims living in the West face hostility and even persecution.[49] As spectacular terror attacks generate considerable fear among the western electorates, ISIL's use of cyber intelligence collection, recruitment, and kinetic attack will elicit louder calls for intensive Internet monitoring to support the counter-terror mission.

Translating desired policies into a real, viable cyber campaign is the unique challenge of the moment. In June 2016, a dissenting memorandum signed by 51 US Department of State diplomats argued for a more rigorous effort to bring about a cessation of hostilities in Syria. While the diplomats argued for, "a more militarily assertive US role in Syria," they preferred to leverage kinetic technologies such as precision-guided weapons and air defense systems for offensive and defensive roles, respectively.[50] The memo stressed a new policy where belligerence by any of the warring parties, i.e. the Syrian regime and ISIL, would be met with force. The question is how cyber forces could be employed to degrade further ISIL's ability to wage war as well as forcing the Assad government to acquiesce to a ceasefire.

Top Pentagon leadership mentioned cyber "bombs" that it wishes to deploy against ISIL.[51] The US military is considering what sort of cyber munitions, capabilities, or tactics might make the most headway in reducing ISIL's battlefield capabilities. The US military must map desired capabilities to an assessment of what is technically feasible now or with varying degrees of effort. There are likely three desired cyber combatant areas in which most activity should fall: intelligence gathering from cyberspace's fixed and mobile computational infrastructure including networks both wired and wireless; cyberattack capabilities designed to degrade or damage battlefield effectiveness of targeted forces; and cyber-information campaigns against enemy messaging.

> Cyber warriors will need to create a capability at the intersection of Silicon Valley and the Pentagon that delivers innovative, unorthodox cyber tools.

While it is impossible to know much of the current US cyber-signals intelligence capabilities without moving into the classified space, we can conjecture on the sorts of capabilities that may be desirable in sweeping up additional intelligence resources. One of the items leaked by Edward Snowden was Tailored Access Operations (TAO),[52] the capacity to gain entry to important systems by either physical or virtual means.[53] What would be enormously useful is to have the capacity for TAO at a distance. Operational units would call upon lightweight off-the-shelf and open source technologies to pull intelligence, map digital points of presence, and see (in real time) data linkages on the battlefield and beyond it. Holding measurement and signatures mapping of the computer terrain might bring useful capabilities in intelligence collection and targeting as well.[54]

While ISIL's combatants are wedded to the same armaments used from conflicts in

Vietnam, Angola, Somalia, and Bosnia, chiefly the Kalashnikov assault rifle and the rocket-propelled grenade, the lure of adopting weaponry that is more sophisticated will likely grow. As the Internet of Things (IoT) extends to vehicles and other tools employed by ISIL and other insurgents, the potential will grow for cyberattacks against them. So far, US security experts have expressed concern over IoT vulnerabilities.[55] While hackers at DEFCON and Black Hat conferences have made news with car hacking, USCYBERCOM should begin thinking about how to get inside the computing components of the Toyota Hilux and Land Cruiser 4x4 vehicles that are key to the mobility of Jihadist elements from Mogadishu to the Maghreb.[56]

Today, as ISIL uses drones, USCYBERCOM should put resources into monitoring or disabling their control systems whether in defensive postures around vital installations such as nuclear power stations or government buildings, denying ISIL the drone intelligence and transport capability on the battlefield.[57] Non-lethal attacks would minimize collateral casualties and reduce insurgent capabilities. The US should accept a Harvey Sapolsky assertion on non-lethal cyber capabilities when he discussed non-lethal ammunition, “The first time a Marine shoots a bad guy with a beanbag, and the bad guy gets up and shoots back, will also be the last time the Marine uses the beanbag.” Nonetheless, there will be no shortage of kinetic hacking targets for the US military.

The cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates.

Also seemingly infinite are the Internet messages supporting ISIL’s war effort. While the platforms—such as Twitter, Instagram, and YouTube—are used to convey Jihadist messaging can police their content to some degree, the US government straddles a fine line in censoring ISIL and other Jihadist groups in cyberspace. The US Intelligence Community (IC) will no doubt continue its work examining social media outlets in a manner not dissimilar from how the Middle Eastern governments overthrown by the Arab Spring sought to accomplish. The key to short-circuiting communications for ISIL may be to borrow the concept of ransomware, the encryption of key data on important systems that have mushroomed into cybercrime. Encrypting stored data or even data in transit that threatens ISIL and its recruitment efforts may be a useful tool. So too might be technical failures of commodity computing hardware triggered by a cyberattack. Think of such tools as Stuxnet for data obfuscation or deletion.

It is important for the US to adopt a culture of innovation that is inclusionary of heterogeneous ideas and actors. The IC has employed its startup venture capital vehicle, In-Q-Tel, to develop desired capabilities where the commercial technology industry has not seen opportunity. As the Cold Warriors employed Lockheed’s Skunk Works to develop world-changing technologies like the U-2, SR-71, and F-117, the cyber warriors will need to create a capability at the intersection of Silicon Valley and the Pentagon that delivers innovative, unorthodox cyber tools and weapons that move from idea to deployment on a schedule far faster than current government acquisition. This would likely take form in a linkage between USCYBERCOM geeks and SOCOM's operators. Much as the US SOF community has developed unique transport, intelligence, and support capabilities, it will need a cyber echelon housed within its intelligence component as well. Already arguments have begun to emerge for a 'Cyber JSOC' (Joint Special Operations Command), the analog to SOCOM's JSOC force composed of Army Delta Force and Naval Special Warfare Development Force (DEVGRU) direct action units as well as its Intelligence Support Activity (ISA).[58]

There will no doubt be difficulties incorporating cyber operations components into overall US strategy countering ISIL and other non-state adversaries; however, it is clear national security leadership in Washington will leverage cyber capabilities more significantly. One issue that will continue to dog offensive cyber operations and intelligence activities is the equities question—should the US government turn over knowledge it accrues regarding cyber vulnerabilities to the technology industry so that they may be repaired. For instance, is it more desirable for USCYBERCOM and the National Security Agency (NSA) to keep information regarding broken encryption implementations or software as was alleged in the Heartbleed bug in the OpenSSL software libraries? Issues such as this will be a major policy question to consider.

Ultimately, the cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates. Looking backward, we can see the effective application of robust signals intelligence capabilities have been. Consider US support of Colombian operations against the Fuerzas Armadas Revolucionarias de Colombia (FARC). There can be little doubt that the Colombian military and police were made significantly more effective with the addition of US intelligence capabilities. Policymakers are keen to eradicate or at least damage ISIL but will need to ask how cyber weapons can frustrate it as much as anything else can. The more cyber tactics can short-circuit ISIL's operational capabilities, the better. What is necessary for US cyber operators are clear objectives from senior leadership on what they want to produce. The engineers that build USCYBERCOM's tools and the hackers that serve as its operational forces can easily enough push back on what they believe is the art of the possible.

Special Contributors

Fernando Barajas, Undergraduate Research Assistant, Rice University

Eric Brittain, Undergraduate Research Assistant, University of Houston

Mamie Sellam, Undergraduate Research Assistant, University of Houston

Jonathan Vallow, Undergraduate Research Assistant, University of Houston

NOTES

1. Pierluigi Paganini, "Mikko Hyppönen Warns the ISIS Has a Credible Offensive Cyber Capability," *Security Affairs,* October 26, 2015.

2. Alireza Nader, *Iran's Role in Iraq,* RAND: Santa Monica, 2015.

3. Thomas Grove and Ben Kesling, "Russia Pursues Ties With Kurds to Keep Foothold in Region," *Wall Street Journal,* April 21, 2016.

4. Eduardo Gonzalez, "Kurdish Peshmerga: Divided from Within," *Harvard Political Review,* September 5, 2015.

5. Adam Taylor, "Why Turkey banned Twitter (and why banning Twitter isn't working)," *Washington Post,* March 21, 2014.

6. James Stavridis, "The New Triad," *Foreign Policy,* June 20, 2013.

7. Michael Eisenstadt, "Defeating ISIS: A Strategy for a Resilient Adversary and an Intractable Conflict," *Policy Notes – The Washington Institute for Near East Policy,* No. 20, November 3, 2014.

8. Jack Moore, "Why air strikes alone can't destroy ISIS," *Newsweek,* December 4, 2015.

9. Hamid Dabashi, "ISIL turns 'shock and awe' doctrine against Islam," *Al Jazeera,* July 5, 2016.

10. Holly Yan, "Showing off its crimes: How ISIS flaunts its brutality as propaganda", *CNN Regions,* September 4, 2014.

11. Sam Webb, "ISIS Use Instagram to Post Sickening Bodycam Footage of Murderous Assault on Civilians in Iraqi City," *Mirror,* May 15, 2015.

12. "ISIS Beheading Four Prisoners," *Zero Censorship,* February 3, 2016.

13. David Goldman, "Twitter goes to war against ISIS", *CNN Money,* February 5, 2016.

14.P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

15. David Blanchette, "Homeland Security Expert: ISIS Thrives on Social Media," *The State Journal-Register,* March 20, 2016.

16. P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

17. Steve Almasy, "Boston Shooting: Who Was Usaamah Rahim?" *CNN U.S.,* June 4, 2015.

18. Ray Sanchez, "ISIS Exploits Social Media to Make Inroads in U.S.," *CNN U.S.,* June 5, 2015.

19. Hassan, "The secret world of Isis training camps – ruled by sacred texts and the sword," *The Guardian,* January 25, 2015.

20. "ISIS Recruits Fighters through Powerful Online Campaign," *CBS News,* August 29, 2014.

21. Olivia Becker, "ISIS Has a Really Slick and Sophisticated Media Department." *VICE News,* July 12, 2014.

22. P. W. Singer and Emerson Brooking, "Terror On Twitter: How ISIS is Taking War to Social Media - and Social Media is Fighting Back," *Popular Science,* December 11, 2015.

23. Francesca Trianni and Andrew Katz, "Why Westerners Are Fighting for ISIS," *Time,* September 5, 2014.

24. Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times,* June 27, 2015.

25. Husna Haq, "ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why (+Video)," *The Christian Science Monitor,* October 22, 2014.

26. John Hall, "European ISIS Fighters Who Are Seen as Cannon Fodder by Their Commanders Desperately Try to Prove Their worth by Committing the Most Sickening Atrocities, Says Former Prisoner," *Mail Online,* April 10, 2015.

NOTES

27. "Isis Leader Encourages Lone Wolf Attacks on Civilians in Europe and US," *The Guardian,* May 22, 2016.

28. C. J. Chivers, "Facebook Groups Act as Weapons Bazaars for Militias," *The New York Times,* April 06, 2016.

29. Jessica Guynn, "Facebook Bans Private Gun Sales," *USA Today,* January 30, 2016.

30. Dave Lee, "Diaspora Social Network Cannot Stop IS Posts," *BBC News,* August 21, 2014.

31. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired,* November 19, 2015.

32. Brendan Koerner, "Why ISIS Is Winning the Social Media War," *Wired,* April 2016.

33. Joseph Marks, "ISIL Aims to Launch Cyberattacks on U.S.," *Politico,* December 29, 2015.

34. Jess Mchugh, "ISIS Cyber Attack? US Government, Planes Threatened With Malware, Hacking By Islamic State," *International Business Times,* December 29, 2015.

35. Jose Pagliery, "ISIS Is Attacking the U.S. Energy Grid (and Failing)." *CNN Money.* October 16, 2015.

36. David Goldman, "Twitter Goes to War against ISIS," *CNN Money,* February 5, 2016.

37. "How ISIS Games Twitter," *The Atlantic,* June, 2014.

38. "ISIS Launches Twitter App For Android Phones," *CBS DC,* June 17, 2014.

39. Anthony Cuthbertson, "Iraq Crisis: Isis Launch Twitter App to Recruit, Radicalise and Raise Funds," *International Business Times,* June 18, 2014.

40. Jose Pagliery, "ISIS is attacking the U.S. energy grid (and failing)", *CNN Money,* October 16, 2015.

41. Lorraine Murphy, "The Curious Case of the Jihadist Who Started Out as a Hacktivist," *Vanity Fair Hive,* December 15, 2015.

42. Lorenzo Francecshi-Bicchierai, "How a Teenage Hacker Became the Target of a US Drone Strike," *Motherboard,* August 28, 2015.

43. Megan Garber, "Doxing: An Etymology," *The Atlantic,* March 6, 2014.

44.Kimiko de Freytas-Tamura, "Junaid Hussain, ISIS Recruiter, Reported Killed in Airstrike," *New York Times,* August 27, 2015.

45. "ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges," *Department of Justice Office of Public Affairs,* October 15, 2015.

46. Joseph Marks, "ISIL Aims to Launch Cyberattacks on U.S.," *Politico,* December 29, 2015.

47. Cory Bennett and Elise Viebeck, "ISIS Preps for Cyber War," *The Hill,* May 17, 2015.

48. Dan Lohrmann, "Cyber Terrorism: How Dangerous Is the ISIS Cyber Caliphate Threat?" *Government Technology,* May 18, 2015.

49. Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times,* June 27, 2015.

50. "State Department Draft Dissent Memo on Syria," *The New York Times,* June 17, 2016.

51. Cory Bennett, "Pentagon hits ISIS with 'cyber bombs' in full-scale online campaign," *The Hill,* April 25, 2016.

52. Andrea Peterson, "The NSA has its own team of elite hackers," *Washington Post,* August 29, 2013.

53. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired,* November 19, 2015.

54. A capability developed or under development by SRC, a defense contractor. "MASINT Systems," SRC, available at: http://www.srcinc.com/what-we-do/radar-and-sensors/masint-systems.aspx.

55. As Nicholas Weaver opined, "I don't do SCADA research because I like to sleep at night." Tom Simonite, *MIT Technology Review,* January 28, 2016.

56. Seth Rosenblatt, "Car hacking code released at Defcon", *CNET Security,* August 2, 2013.

57. David Hambling, "ISIS Is Reportedly Packing Drones With Explosives Now," *Popular Mechanics,* December 15, 2016.

58. "U.S. Needs 'Cyber JSOC' So It Can Strike Harder, Faster In Event Of Conflict: Experts," *CyberWar.News,* April 27, 2016.

Bridging the Cyber-Analysis Gap: The Democratization of Data Science

John Healy
Leland McInnes
Colin Weir

ABSTRACT

The challenges of ever growing and ever changing Big Data are broad and far-reaching, particularly in the cyber-defense domain. The task of analyzing and making sense of this data is difficult, and only getting worse. We propose that by democratizing data science and making it accessible to everyone, we can expand the breadth and depth of analytics available to a point where we can potentially meet the challenges of Big Data.

THE ONCOMING WAVE OF BIG DATA

As computing and sensor facilities become ever more pervasive and interconnected, the amount and diversity of data available to cyber-analysts continue to grow at an exponential rate. The cyber-analyst's ability to analyze and leverage all the data is currently lacking. The tools available to analysts do not scale to the volumes of data we have now, let alone the volumes which are expected in the future. This is a significant challenge that must be addressed by current and future cyber-defense organizations.

To face the challenges of ever growing data, the data science community needs to empower cyber-analysts with more intelligent tools. We need tools that provide complex, nuanced analyses and intelligent summarizations of the data. Such tools are the domain of machine learning and data science. This growing field can provide powerful models for analyzing data. For example, analyses capable of automatically determining the state actor behind a newly discovered piece of malware, or tools capable of automatically detecting and blocking malicious web traffic never previously identified. Since analytic tasks are incredibly diverse and always changing to respond to new data, the cyber-analyst community needs machine learning tools that are general and flexible enough to cope with this evolving diversity. This might appear to require something more general than the narrow intelligence that traditional machine learning provides. We claim that this is not the case.

John Healy, Leland McInnes and Colin Weir are senior researchers at the Tutte Institute for Mathematics and Computing in Ottawa, Canada. The Tutte Institute brings together leading researchers from academia, industry and government to solve the most challenging classified and unclassified problems facing the security and intelligence community. The authors exemplify this cross-disciplinary approach, with diverse backgrounds in pure mathematics, computer science, statistics, machine learning, and cyber-security. Combined, the authors have eight advanced degrees and over 40 years of research experience spanning the gamut of government, industrial, and academic positions.

The functionalist school of philosophy of mind holds that human intelligence is merely the composition of a vast array of specialist systems [Den92, Den98, Den06]. This composite has no central point of control but is instead a swarm of specialist systems that are continuously co-operating, competing, and interacting. Such a system potentially provides the generality and flexibility of human intelligence without ever having a singular general intelligence. This provides a compelling analogy for how many interacting specialists models can come to provide a whole that is greater than the sum of their parts. We propose that the solution to the ever changing diversity of data lies in a vast army of models. Each model can be highly specialized but, with enough interacting models, a great diversity of tasks can be easily accomplished. The ecosystem of models is *smarter* than any individual model. This is "the wisdom of the crowd" writ nanoscale ([Gal07]).

Currently, building computational predictive models is the domain of machine learning experts. This is a bottleneck on model construction and on deployment to cyber-analysts. Most tellingly, it puts significant constraints on the latency of cyber-analyst feedback for improving or specializing models. In a world where every analyst can build their own machine learning models, specialized to their own needs, this feedback loop is dramatically tightened. A model can efficiently be tailored to each analyst's specific needs, offloading cognitive tasks to the machine, and a small army of analytic models can quickly be promulgated among analysts in a shared collaborative workspace. With such a system of co-operating, competing and interacting models, the system-as-a-whole begins to resemble functional machine intelligence.

In this view, our goal is not to build ever more complex and general models. Instead, the answer lies in democratizing machine learning and making it pervasive. The Internet changed the world by democratizing data generation: data was no longer sequestered in carefully controlled databases, but generated by everyone, everywhere, all the time. To build the dynamic ecology of machine learning models that we propose, we need to democratize data analytics and put the power of machine learning directly in the hands of analysts. Thus, the question we should be asking is "how can we transform the technological landscape to make machine learning and data science ubiquitous?"

TRANSFORMATIVE TECHNOLOGIES AND THE END OF DATA SCIENCE

Simple technologies can have remarkable transformative powers, fundamentally changing the landscape of ideas. A simple example of this kind of subtle revolution is the development of spreadsheet software. The first real spreadsheet program was VisiCalc, developed by Dan Bricklin and Bob Frankston in 1979. The concept was simple, elegant and seems, on reflection, obvious: allow data to be entered in rows and columns and allow arithmetic formulas to be computed across those rows and columns. Most importantly, if a data entry is changed, then the change should propagate through the formulas and be instantly visible to the user. VisiCalc was an instant success and became a driving factor in the rise of personal computers: for many buyers, VisiCalc was the motivating reason to purchase a computer! By the mid-1980s spreadsheets were everywhere, and the market was dominated by Lotus 1-2-3, which integrated charting and plotting to spreadsheets. Spreadsheets became so central that, on the first release of Microsoft Windows, Excel was the flagship product designed to draw users to the fledgling operating system ([Pow04]).

To face the challenges of ever growing data, the data science community needs to empower cyber-analysts with more intelligent tools.

What was the change that spreadsheets spurred? They powered the first data revolution. As long as data lived in carefully curated databases on distant mainframes, it remained sparse. Once it became possible to create and work with data locally and visually via spreadsheets, the amount of data generated exploded. Spreadsheets made it possible for everyone to work with data, and so everyone did. Data was entered, plotted, linked and transformed on a scale never seen before. In short, spreadsheets changed the very way people look at and think about data—it became something that everyone has, and everyone can use. The expansion of data enabled by spreadsheets was but the first ripples of the oncoming wave of Big Data. With the democratization of data generation provided by the Internet, data has grown far beyond the analytic power of spreadsheets, and we are only seeing the early warning signs of a wave of data that threatens to wash us away.

With the arrival of internet-connected sensor networks and the Internet of Things, both the cyberattack surface and associated data will quickly grow far beyond our limited data-analytic capabilities. We need a second data revolution. Spreadsheets provided arithmetic analytics and visualization; today the cyber-analyst community needs radically new ways to summarize the immense volumes of data at their disposal—the next wave in the data revolution appears to be driven by machine learning analytics.

The second data revolution will arrive with new tools and new transformative technologies. The keys to the success of spreadsheets were their low barrier to entry, their remarkable versatility, and the powerful tools that could be built with them. With data now beyond the scope and capability of spreadsheets there is a need for new tools that ask a little more of the user, but exponentially increase versatility and analytic power. When spreadsheets were unleashed upon the world computers were a foreign concept to most, so the extremely straightforward and visual interface provided by VisiCalc was critical. Now, however, computing is pervasive, and with movements like code.org [Cod15] and President Obama's "Computer Science for All" initiative [Smi16], basic programming skills are rapidly becoming part of the mandatory curriculum ([Nor16], [Wat16]). We no longer need to assume users are unable to cope with simple programming tasks, and this opens up a vast untapped wealth of flexibility and power. Under this rubric, the transformative tools that are needed are already on the horizon.

Much of the open-source community, faced with the requirements for Big Data analytics, is consolidating on infrastructure to power the human-computer interface for data analytics. For example, the Jupyter notebook interface ([Jup16c]) provides rich tools for interactive programming. Notebooks are living interactive documents that contain explanatory text, live code, visualization, and rich visual display of interactive content. The versatility of the system is incredible ([GP15, She14, Jup16a, Jup16b]) while still providing a simple and intuitive interface. From the convergence of the pervasive programming skills of the coming generation and the powerful visual interface of tools such as Jupyter, the cyber-analyst community can expect a transformation of analysis tools from the outdated and ill-equipped to a shared collaborative ecosystem of living notebooks.

If tools similar to Jupyter provides the surface interface, what can provide the substrate? Python is the lingua franca of data science and machine learning.[1] It has spawned a growing ecosystem of data analytics and machine learning tooling built upon it (including Jupyter itself). This is an open-source ecosystem, and, in the spirit of the source language, focused on intuitive ease of use ([Pet04, Oli15]). The result is not a product, but a collaboratively built platform: data science tools by the masses for the masses. This is the democratization of data analytics underway as we speak.

In short, the second data revolution is almost upon us. Powered by machine learning, soon to be accessible to all in a vast collaborative workspace of notebooks, the cyber-data challenges of the future will be tamed—not by specialist data scientists, but by shared efforts of ordinary analysts, newly empowered by transformative tools. Data science will become so pervasive, so ingrained in every mind that it will cease to exist as a separate concept. Much like the spreadsheet, we won't be able to imagine a world without it.

THE WHOLE IS MORE THAN THE SUM OF ITS PARTS

In 2001, a small upstart encyclopedia arrived to challenge the reign of *Encyclopedia Britannica.* At the time, *Wikipedia* seemed like a toy project, without any of the expert research and editing staff available to a giant like *Britannica.* Instead, *Wikipedia* has come to completely eclipse any other encyclopedia on the planet for both the breadth and depth of knowledge that it successfully captures and presents. It achieved this remarkable feat by democratizing the task of compiling human knowledge through the wisdom of the crowd. Anyone with access to a computer can use and edit Wikipedia. The feedback loop is swift—if you see something wrong or that can improve you can edit it immediately and see the results. Better still, everyone else also immediately sees the results of your edit and can adapt it, comment on it, or revert it. With enough people making edits, the text slowly but surely lurches its way toward a consensus description of the topic at hand. No single edit is necessarily *right*, nor final. The result is something better than any of its individual authors may have produced. In short, *Wikipedia* is more than the sum of its edits.

At the Chesapeake Large Scale Analytics Conference, a survey of attendees demonstrated that the expected time-frame for delivery of a new predictive analytic model to production was three months and could often be as long as a year or more. That represents a delay of months, or even a year before front-end analysts can evaluate the usefulness of the model on current, real-world data. For problems that remain relatively stable over time, this may be a reasonable approach. In the dynamic adversarial world of cyber-defense, such a delay is potentially devastating. Dramatically shrinking the cyber-analyst feedback loop on models and enabling a *fail-fast* approach is critical to the wider success of machine learning in cyber-analytics. To do this, we need to embrace the democratizing approach and rapid feedback that made *Wikipedia* so successful.

> In this view, our goal is not to build ever more complex and general models. Instead, the answer lies in democratizing machine learning and making it pervasive.

As we have already seen, Jupyter and Python provide a powerful infrastructure for collaborative data science for analysts. Furthermore, with robust machine learning tools the data science community can empower cyber-analysts to make use of state of the art machine learning. Bringing all of this together in a shared collaborative workspace can enable analysts to co-operatively develop machine learning models and analytics. The result of this confluence of technologies is an open and flexible ecosystem that can evolve and grow with analysts' needs. This will require further development of the software infrastructure, however, with sufficient work, it can become the *Wikipedia* of data analytics, with a breadth and depth of models and analysis that eclipses anything that has come before. It can be an analytic platform that is far more than the sum of its models.

MACHINE LEARNING THAT JUST WORKS

Cars have existed, in various forms, since the late 18th century [Eck01]. Despite their long history, it wasn't until the 20th century that cars became the transforming societal force that they are today. The catalyst for that transition was the introduction of the Ford Model T. In the year that the Model T was introduced the world land speed record was held by a car—a steam powered car. This was the car technology of the 18th century with literally centuries of steady improvements and refinements creating a finely tuned, precision engineered racing machine. Ford's genius was realizing that car design had been solving the wrong problem. High end, high-performance cars were both expensive, and temperamental. In contrast, the Model T was not designed to be the best, nor fastest, car, but a car that was inexpensive and reliable. By making the car available to everyone Ford democratized personal transport, and in so doing disrupted the entire industry and changed the world.

> Simple technologies can have remarkable transformative powers, fundamentally changing the landscape of ideas.

Machine learning has been around since the 1960s and has made many remarkable advances in that time. More recently machine learning has become a competition; from the KDD Cup ([KDD16]) and the Netflix Prize ([Net07]) to the ImageNet Challenge ([Ima15]) and Kaggle ([Kag16]). The metric for all these competitions is model accuracy. Model accuracy is the land speed record of machine learning. The models produced are near miraculous in their accuracy, but are also extremely complex and intricate, requiring considerable expertise to build and maintain. What is needed for today's analysts are machine learning tools that make model construction inexpensive and reliable—without necessarily optimizing solely for model accuracy. Simple, robust models would bring the power of machine learning to the masses. This is a different approach to designing machine learning tools and algorithms, and deserves significant research effort—since the result, the democratization of machine learning will be as revolutionary as the democratization of transport enabled by Ford's Model T.

Inexpensive, robust models are also required for machine learning in production environments. In 2014 Google published a highly influential paper titled *Machine Learning: The High Interest Credit Card of Technical Debt* [SHG + 14]. The primary thesis was that while machine learning was extremely powerful and could bring quick wins, it could also prove to be a maintenance nightmare. This was predicated on intricate traditional machine learning models which, due to their expert tuning and calibration, were hard to modify or update. On the other hand, if democratized robust models are used the problem evaporates. Models that are inexpensive to build are disposable—this accumulates very little debt, it is paid down by simply building a new model. We are even beginning to see such thinking taking hold in practice: the winning Netflix Prize entry was not implemented at Netflix due to its complexity and the vast amount of delicate hand tuning—a much simpler to maintain a model that was mere fractions of a percentage point less accurate was deemed to be the most effective solution.

The move from complex traditional models to simple practical models can be achieved by a directed research program on techniques for robust models. The foundation for such a research program is already beginning to take shape. The generalized low-rank model framework ([UHZB15]) from Stanford provides a powerful and general framework for automated feature engineering. Random Forest models ([Bre01]) provide classification models that 'just work'. Recent advances in clustering ([CMAS15, CM10]) show promise for robust unsupervised learning, including anomaly detection. Neural network motivated techniques such as word2vec and GloVe ([MCCD13, PSM14]) offer a foundation for research into text analytics for the masses. Building upon this work to fill out a complete set of machine learning tools that *just work* will bring robust models to the heart of machine learning research.

We claim that the resulting increase in both the scope and the power of analytics can meet the challenges of the ever-growing and ever changing data landscape of cyber-analytics.

An immediate proposal for such democratization might look like a shared ecosystem of Jupyter notebooks overtop of Python and its suite of rapidly developing tools. A small cadre of more technologically literate cyber-analysts could be trained with minimal effort to be able to leverage the machine learning models of data science in their everyday work. In the longer term, research into more intuitive and powerful techniques and languages along with an increase in general programming literacy may alter this framework and help to both empower and reduce the cognitive load upon the broader analyst community.

Ultimately our proposal is to bring ordinary analysts and machine learning closer together. This involves trained cyber-analysts working with machine learning techniques designed specifically for cyber-analysts, bridging the gap by bringing each closer to the other. Closing this gap remarkably expands the user base of machine learning and data science, and shrinks the feedback loop allowing rapid evolution of models and analytics. In turn, this is a catalyst creating an ever-growing breadth and depth of analytic capabilities. We claim that the resulting increase in both the scope and the power of analytics can meet the challenges of the ever-growing and ever changing data landscape of cyber-analytics.

NOTES

1. Other languages such as R and Julia compete in this space, but currently the momentum is with Python in the machine learning (as opposed to general statistics) fields – see scikit-learn and tensorflow for examples.

NOTES

[Bre01] Leo Breiman, Random forests, *Machine Learning,* 2001.

[CM10] Gunnar Carlsson and Facundo Memoli, Multiparameter hierarchical clustering methods, *In Classification as a Tool for Research,* 63–70, 2010.

[CMAS15] R.J.G.B Campello, D. Moulavi, A.Zimek, and J. Sander, *Hierarchical density estimates for data clustering,* ACM Transactions on Knowledge Discovery, 1–51, 2015.

[Cod15] Code.org https://www.code.org, 2016.

[Den92] Daniel C. Dennett, *Consciousness Explained,* Back Bay, 1992.

[Den98] Daniel C. Dennett, *Brainchildren: Essays on Designing Minds,* Bradford, 1998.

[Den06] Daniel C. Dennett, *Sweet Dreams: Philosophical Obstacles to a Science of Consciousness,* Bradford, 2006.

[Eck01] Erik Eckermann, *World History of the Automobile,* 2001.

[Gal07] Francis Galton, *Vox Populi,* Nature, 75, 450–451.

[GP15] Brian Granger and Fernando Perez, *Computational Narratives as the Engine of Collaborative Data Science,* https://archive.ipython.org/JupyterGrantNarrative-2015.pdf, 2015.

[Ima15] ImageNet Challenge, https://www.image-net.org/challenges/LSVRC, 2015.

[Jup16a] Jupyter Dashboards, https://github.com/jupyter-incubator/dashboards, 2016.

[Jup16b] Jupyter Kernel Gateway Bundlers, https://github.com/jupyter-incubator/kernel_gateway_bundlers, 2016.

[Jup16c] Jupyter Project, https://www.jupyter.org, 2016.

[Kag16] Kaggle, https://www.kaggle.com, 2016.

[KDD16] KDD Cup Archives, https://www.kdd.org/kdd-cup, 2016.

[MCCD13] Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffery Dean, *Efficient estimation of word representations in vector space,* arXiv, 2013.

[Net07] Netflix Prize, https://www.netflixprize.com, 2007.

[Nor16] Anna North, *Should We All Learn to Code,* http://op-talk.blogs.nytimes.com/2014/06/17/should-we-all-learn-to-code/?_r=0, 2016.

[Oli15] Travis Oliphant, *Python as the Zen of Data Science,* http://youtube.com/watch?v=mNvPiV37F7Q, 2015.

[Pet04] Tim Peters, *The Zen of Python,* http://www.thezenofpython.com, 2004.

[Pow04] Power, D. J., "A Brief History of Spreadsheets", DSSResources.COM, http://dssresources.com/history/sshistory.html, version 3.6, 08/30/2004.

[PSM14] Jeffery Pennington, Richard Socher, and Christopher D. Manning, Glove: *Global vectors for word representation,* In Empirical Methods in Natural Language Processing, 1532–1543, 2014.

[She14] Helen Shen, *Interactive notebooks: Sharing the code,* Nature, 515:151–152, 2014.

[SHG + 14] D. Sculley, Gary Holt, Daniel Golovin, Eugene Davydov, Todd Phillips, Dietmar Ebner, Vinay Chaudhary, and Michael Young, *Machine learning: The high interest credit card of technical debt,* In SE4ML: Software Engineering for Machine Learning (NIPS 2014 Workshop), 2014.

[Smi16] Megan Smith, *Computer Science for All,* https://www.whitehouse.gov/blog/2016/01/30/computer-science-all, 2016.

[UHZB15] Madeleine Udell, Corrine Horn, Reza Zadeh, and Stephen Boyd, *Generalized low rank models,* arXiv, 2015.

[Wat16] Jackie Wattles, *GE CEO Jeff Immelt says all new hires will learn to code,* http://money.cnn.com/2016/08/04/technology/general-electric-coding-jeff-immelt/, 2016.

Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence

Major Michael Kolton

INTRODUCTION

On December 31, 2015, Chinese officials announced a substantial reorganization of the armed forces. [1] The reforms cut across the entire People's Liberation Army (PLA),[2] and constitute the most dramatic reorganization of China's armed forces since the 1950s. [3] President Xi Jinping described the reforms as essential for modernizing the military. [4] and the reorganization affirmed the PLA's fidelity to the Chinese Communist Party (CCP). [5] The reform also established a new service branch called the Strategic Support Force (SSF) on par with the Army, Navy, Air Force, and Rocket Force. Among its many missions, the SSF secures electromagnetic space and cyberspace. [6] China's military pundits lauded the SSF as necessary for twenty-first century warfare. [7] For years, the PLA has fielded cyber capabilities at various levels of command, and the SSF elevates control of cyber operations to the highest echelons. [8] Ultimately, the PLA employs cyber forces to ensure cyber sovereignty *(wangluo zhuquan)* and safeguard the *Chinese Dream* across all domains.

This paper examines China's military cyber activities in three parts. First, the paper attempts to identify China's strategic objective in cyberspace. Second, it outlines one interpretation of China's cyber strategy. Finally, the paper explores the efficacy of US cyber deterrence given China's cyber strategy. PLA cyber doctrine remains abstruse, and public literature does not offer a stand-alone cyber strategy document that articulates the purpose of Chinese cyber operations. Leveraging PLA texts and other publicly available literature, this paper offers one possible reading of China's cyber strategy. In the end, the paper highlights some implications for US-China cyber relations and encourages efforts to build mutual understanding on both sides of the Pacific.

Michael Kolton is a US Army major currently assigned as a graduate student at Yale University’s Jackson Institute for Global Affairs. He is a US Army Foreign Area Officer (FAO) specializing in China. Prior to his current specialty, Major Kolton served as an infantry officer with deployments to Iraq and Afghanistan. He holds a master’s degree in economics from the University of Hawaii at Manoa and a Bachelor’s degree in economics from the United States Military Academy at West Point, New York.

PART 1: CYBER SOVEREIGNTY

Based upon a review of public statements and documents, China’s cyber strategy appears determined to achieve cyber sovereignty; this end unifies the country’s cyber activities. Dr. Lü Jinghua of the Center on US-China Defense Relations at the PLA Academy of Military Science’s (AMS) describes cyber sovereignty as the foundation for a new international code of conduct for cyberspace *(wangluo kongjian xingwei zhunze)* in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace.[9] At the 2012 World Conference on International Telecommunications, China and a majority of attending countries advocated for national governments to boost their control of the Internet.[10] The US and its allies foiled this campaign and upheld the status quo multistake holder approach, which invites participation from civil society, private enterprise, national governments, and international organizations. This conflict of ideas remains an ongoing geopolitical dispute that will define the future of cyberspace.

While the US and others applaud freedom on the Internet, the CCP worries about its latent power to destabilize social and political order.[11] When Chinese academic researchers examined the use of social media to organize street protests in Iran and China’s Xinjiang, they concluded the US will leverage such technologies to spur regime change in other countries.[12] To mitigate these types of perceived Internet risks, China’s Great Firewall blocks sites like Google, Facebook, Twitter, and YouTube.[13] In March 2016, Chinese authorities increased efforts to shutdown virtual private networks (VPNs) that enable citizens and foreign residents to bypass censors.[14] The US government deems an open Internet that transcends national boundaries essential for freedom and prosperity. Yet, Beijing balks at Washington's ideals, and Chinese officials consistently slate US policies on cyberspace governance. There is little reason to believe Beijing will compromise on cyber sovereignty because it seeks unrivaled CCP authority over its citizens in the virtual world.[15]

China's displeasure with the status quo of Internet governance

China's vision for cyber sovereignty imagines cyberspace as a new world for nations to stake their claims. In February 2016, the CCP central committee labeled cyberspace the new frontier of the modern state *(xiandai guojia de xinjiangyu)* and a new arena for global governance *(quanqiu zhili).*[16] Deputy Director of the PLA's National Defense University (NDU) Colonel Li Minghai argues controlling cyberspace *(zhangwo zhi wang quan rutong)* is the twenty-first century equivalent of controlling the maritime domain in the eighteenth century or controlling the air domain in the twentieth century.[17] Colonel Li's historical analogy summons a powerful memory among Chinese readers. British dominance of the high seas allowed European powers to subjugate the Qing Dynasty, and many Chinese citizens still chafe under US Navy patrols of global sea-lanes—especially the South China Sea. Given China's collective trauma from past imperialism, the PLA will not allow history to repeat in cyberspace; it will defend China's sovereignty in the cyber domain.

For decades, the Internet has relied on US-centric architecture in both a technical and organizational sense. In 1998, "a few individuals, a few private standards bodies, several corporations, and the U.S. Department of Commerce" established the Internet Corporation for Assigned Names and Numbers (ICANN).[18] As a California-based, non-profit entity, ICANN pioneered multistakeholder Internet governance beyond the traditional purview of national jurisdictions.[19] In the multistakeholder model, leaders from civil society, private enterprise, and governments collectively determine the rules of Internet operations, which in turn shape the fundamentals of cyberspace. To fulfill its global mandate as facilitator of a free and open Internet, ICANN adopted a charter with by-laws that promote inclusivity and openness.[20]

The PLA employs cyber forces to ensure cyber sovereignty and safe-guard the Chinese dream across all domains.

Over the years, national governments have objected to the Internet's seemingly US-oriented bias. In 2013, Edward Snowden revealed prolific National Security Agency (NSA) surveillance activities, and countries like Brazil and Germany enacted privacy protections that could undermine the Internet's global interconnectivity.[21] A 2015 pro-government Chinese editorial board ridiculed America's so-called "free flow of information" as a ploy to "gather information from around the world, through legitimate and illegitimate means."[22] China and Russia exploited the global controversy surrounding

NSA surveillance to push their model of Internet governance, which cedes control of key Internet operations to national governments.[23]

In light of China's pursuit of cyber sovereignty, September 2016 may prove to be a decisive point for its cyber strategy. For over a decade, the Department of Commerce's National Telecommunications & Information Administration (NTIA) managed a component of Internet operations under contract with ICANN's Internet Assigned Numbers Authority (IANA).[24] In September, NTIA's contract with IANA expired, and the NTIA transferred IANA stewardship to ICANN.[25] The transition raised concerns about the durability of multi-stakeholder governance. Some experts fear an impotent ICANN untethered from US underwriters could gradually allow national governments to compartmentalize cyberspace and sunset the age of free flowing information.[26]

To mitigate perceived Internet risks, China's Great Firewall blocks sites like Google, Facebook, Twitter, and YouTube.

At the November 2016 World Internet Conference, the Cyberspace Administration of China (CAC) endorsed global Internet rules that respect "national sovereignty in cyberspace." Bruce McConnell of the EastWest Institute interprets "national sovereignty in cyberspace".[27] as a noteworthy evolution away from China's controversial pursuit of cyber sovereignty. He explains, "The new language expresses more clearly the obvious point that states should and will exercise responsibility to make cyberspace safer and more secure within their borders ... it removes the impression that any state should seek hegemony in global cyberspace."[28] In this way, McConnell echoes China's long-standing official position on cyberspace governance. On the other hand, a conciliatory tone does not signal a deviation from China's pursuit of cyber sovereignty. China will likely leverage shifts in governance (e.g. the ICANN handover) to shape cyberspace norms.

The importance of cyberspace in twenty-first century warfare

The spirited debate over Internet governance arises from the strategic importance of cyberspace in the twenty-first century. Some PLA theorists believe information age warfare *(xinxi shidai de zhanzhang)* requires militaries to conduct a new hybrid-form of warfare that combines cyber power and firepower. Accordingly, Colonel Li argues cyberspace operations *(wangluo kongjian zuozhan)* will determine victors on twenty-first century battlefields.[29] Therefore, the argument goes, the PLA must build a joint cyber force ready to fight and win future wars.[30] Cyber operations are critical capabilities for national defense, and the PLA cannot allow foreign powers to define the country's future.[31]

In many ways, cyber capabilities have evolved faster than the frameworks leaders rely on to employ them. On April 5, 2016, Admiral Michael Rogers of U.S. Cyber Command (USCYBERCOM) recommended his organization be elevated to a fully unified combatant command.[32] In December 2016, Congress voted to follow such recommendations when it passed the 2017 National Defense Authorization Act (NDAA).[33] The ongoing evolution of China's SSF and USCYBERCOM demonstrate the nascent state of cyber warfare institutions. Chinese and American views of military deterrence also differ, and divergent theories of cyber warfare underscore the importance of ongoing US-China efforts to build norms of behavior in cyberspace. Today's embryonic military cyber doctrines carry risks of bilateral misunderstandings, especially when militaries operationalize cyber deterrence strategies.

At such a pivotal moment in military affairs, mutual understanding between two of the world's great powers is essential for peace. In December 2015, US and China envoys launched a new cybersecurity dialogue to foster mutual understanding that included discussions about confidence-building measures for deescalating tensions.[34] The dialogue followed the September 2015 summit between Presidents Obama and Xi that promised to ease tensions after a string of high-profile cyberattacks.[35] In March 2016, Obama met his counterpart and reiterated China's responsibility to reduce cyber industrial espionage.[36] On December 7, 2016, Attorney General Loretta Lynch, Homeland Security Secretary Jeh Johnson, and Chinese State Councilor and Minister of Public Security Guo Shengkun co-chaired the third US-China joint dialogue on cybercrime. In its joint summary, the US and China committed to "further solidifying, developing, and maintaining the Dialogue mechanism and continuing to strengthen bilateral cooperation in cybersecurity.".[37] At a minimum, these meetings reveal the importance both countries place on cybersecurity.

The PLA will not allow history to repeat in cyberspace; it will defend China's sovereignty in the cyber domain.

Both the US and China trumpet the strategic importance of cyberspace. In its 2006 *Quadrennial Defense Review* (QDR), the US military recognized China's ambitions in cyberspace and its increasingly sophisticated cyber capabilities.[38] In 2014, the Pentagon reaffirmed "the importance of cyberspace to the American way of life—and to the Nation's security."[39] Similarly, China's military has recognized security imperatives in cyberspace. In 2006, the PLA Daily called cyberattacks a serious threat to national security. Cyber operations reshape the security environment by eroding traditional, geographical boundaries *(dili shang de fen jiexian).* By 2025, China must therefore seize strategic opportunities *(zhanlüe jiyuqi)* to ensure a stable security environment in which electromagnetic spectrum and cyberspace constitute the "fifth-dimension of the battlefield." This "fifth dimension" trope parallels the US military's concept of the cyber domain,[40] the global manmade realm within the informational environment that adds on to the four physical domains of air, land, maritime, and space.[41]

To convey foundational principles for cyber operations, American and Chinese experts have evoked various analogies to describe the informational environment and articulate military imperatives. For example, American and Chinese military writers have both used "cyber terrain" metaphors to express cyber operations.[42] In such analogies, key cyberspace terrain equates to the proverbial high ground on physical battlefields, which militaries must seize in order to dominate an adversary.[43] For example, Senior Colonel Ye Zheng of AMS calls cyberspace the new high ground *(quanxin zhigaodian)* for national sovereignty.[44]

Some PLA theorists believe information age warfare requires militaries to conduct a new hybrid-form of warfare that combines cyber power and firepower.

Military dominance in cyberspace remains a strategic task for the PLA. To obtain cyber sovereignty, the PLA must identify key terrain for its cyber forces to seize, control, and retain. Deputy army commander of the PLA 16th Group Army, Major General An Weiping, argues the PLA must build cyber forces that can "seize the high ground in military competition and win information-based battles."[45] Major General An views cyberspace as "an important battlefield to obtain the information supremacy and a strategic means to obtain asymmetrical advantages."[46] Across all domains, the general expects to employ cyber operations to safeguard national security.[47] Major General An believes cyber operations like the Stuxnet attack on Iran's nuclear centrifuges necessitate developing China's joint cyber forces.[48] In this way, the SSF is a manifestation of China's anxieties over superior US military capabilities.

Since 2006, both militaries have fielded increasingly sophisticated cyber capabilities while refining policies and doctrine to guide their employment. Amid such a fast-paced evolution in military affairs, adversaries understandably struggle to interpret one another's intentions. The secretive nature of security decision-making further undermines the accuracy of predicting an adversary's intent.[49] Moreover, another country's security decisions occur within its specific cultural context, which further confuses political or military signals between powers.[50] Military doctrine differs between China and the US, and this incongruence in cyber doctrine exacerbates the risk for miscalculations and escalation.

Irreconcilable differences

Although the US and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world. The Atlantic

Council's Jason Healey calls this divergence "a bifurcation between east and west" that allows little room for compromise.[51] Testifying before Congress in 2015, Assistant Commerce Secretary Lawrence Strickling defended America's support for multi-stakeholder Internet governance. As head of the NTIA, Strickling implicitly criticized China and Russia for pursuing greater control over the Internet.[52] Beijing rejects the ideal of an open Internet, and it has found likeminded leaders in Moscow.[53] The CCP wants to govern its citizens in cyberspace with the same authority it exercises in the physical realm.[54]

Admittedly, China's cyber sovereignty approach does hold national governments accountable for the behavior of their citizens. Such a direct accountability could incentivize laggard countries to more enthusiastically tackle cybercrime originating from within their borders.[55] Despite this potential benefit, the US believes multistakeholder governance underwrites Internet freedom and protects the innovative ecosystem that drives prosperity. The US rejects China's push for a new multilateral approach.

Today's embryonic military cyber doctrines carry risks of bilateral misunderstandings, especially when militaries operationalize cyber deterrence strategies.

Beijing meanwhile remains firmly opposed to the US position. On December 16, 2015, Xi Jinping called upon the international community to "respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."[56] In a not too subtle critique of the US, Xi said, "Existing rules governing cyberspace hardly reflect the desires and interests of the majority of countries."[57] The CCP repudiates cyberspace norms that undermine its authority to govern the Chinese people. Colonel Ye Zheng of AMS explains:

> To achieve cybersecurity requires 'cyber rules.' Rules are the basis of order, and order is the basis of security. The core of cybersecurity is to establish cyber rules and implement them. Without cyber rules, activities in cyberspace will be out of control, cybercrimes will be rampant, and cybersecurity will be harmed. Cyberspace is now in a disordered state because no actions have been taken to develop cyber rules and there is no international consensus about how to work out the rules.[58]

China has long combined political, economic, diplomatic, and military elements to defend its sovereignty.[59] Notwithstanding US and European opposition, China and Russia appear firmly committed to pursuing their goal of cyber sovereignty.[60] US and China cyberspace policy goals likewise appear destined for perennial conflict. Beijing has demonstrated a dogged pursuit of cyber sovereignty despite objections from the US and its allies.

PART 2: CHINA'S PLA CYBER STRATEGY

Before we can identify the PLA's cyber strategy, we must understand the national policy goals that guide China's armed forces. The values of a country shape its vision for cyberspace, which then guides national policy and military strategy. On the first page of its 2015 *Cyber Strategy,* the US military declares, "The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. These qualities of the Internet reflect core American values—of freedom of expression and privacy, creativity, opportunity, and innovation."[61] In China, the chief goals of its 2015 draft national cybersecurity law are (1) ensure cybersecurity, (2) safeguard cyberspace sovereignty, national security, and the public interest, (3) protect the legitimate rights and interests of citizens, legal persons and other organizations, and (4) promote the healthy development of economic and social information.[62] These themes from China's cybersecurity law persist across various official publications. Instead of an open and free Internet, China emphasizes security and sovereignty. The US and China differ in their vision for cyberspace, and their subsequent strategies reflect this divergence.

The Chinese Dream: China's national policy objective

Importantly, the PLA safeguards China's national strategic goal of the "Chinese Dream" *(zhongguomeng).*[63] Soon after becoming party secretary in 2012, Xi described the Chinese Dream as collective rejuvenation—a revival of prosperity, unity, and strength.[64] In a 2015 interview with the *Wall Street Journal,* Xi explained that in order to understand the Chinese Dream "one needs to fully appreciate the Chinese nation's deep suffering since modern times and the profound impact of such suffering on the Chinese minds."[65] Under the custodianship of the CCP, the country pursues the Chinese Dream through resurgent national strength free from foreign interference.

> Although the US and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world.

In May 2015, China's Ministry of National Defense (MND) published a white paper articulating the country's military strategy. The document reimagined military power and entreated the PLA to abandon its "traditional mentality" focused on land warfare.[66] Major General Chen Zhou described the white paper as call for the PLA to adapt to new political-security realities and build a modern military force.[67] A Chinese commentator called the MND white paper the most transparent report of PLA strategy in thirty years.[68] Yang Yucai, professor of strategy at China's NDU, said the document clearly articulates the country's strategic aims.[69] Anthony Cordesman and Steven Colley of the Center for Strategic and International Studies (CSIS) likewise accept the white paper as a conduit for understanding PLA strategic thinking.[70] Admittedly, such publications judiciously reveal information and fail to confirm which concepts the PLA operationalize and which ones they reject.[71] PLA texts do not necessarily reflect views from the whole of Chinese government.[72] Nevertheless, the MND white paper helps examine PLA strategic thinking.

The PLA is an instrument of military policy in service to the CCP and the state.[73] In this light, the PLA must fulfill its mandate *(lüxing shiming)* as the Party's army,[74] and the armed forces must always obey the Party.[75] Strategic goals *(zhanlüe mudi)* determine military decisions, and leaders design strategy and develop doctrine that serves the CCP.[76] The PLA evaluates success by achieving the CCP's political objectives.[77] For example, the CCP expects the PLA to guarantee "a stable external environment for continued economic development."[78] Major General Chen Zhou, director of the National Defense Policy Research Center at AMS, summarizes PLA ethos with a traditional Chinese axiom: military affairs must comply with the needs of politics, and military strategy must comply with the requirements of the country's political strategy *(junshi fucong zhengzhi, zhanlüe fucong zheng'e).*[79] Thus, military strategy must support simultaneous efforts across the whole of government to achieve the CCP's strategic end state.

The Chinese Dream orients China's government across numerous concurrent efforts. The 2015 Military Strategy explains, "China's armed forces take their dream of making the military strong as part of the Chinese Dream. Without a strong military, a country can be neither safe nor strong."[80] China identifies an advanced military as a strategic means *(zhanlüe shouduan)* for accomplishing strategic ends *(zhanlüe mudi).* As the country aims for the Chinese Dream, the strategic end-state for the PLA can be expressed in three sub-objectives: sovereignty, modernity, and stability.[81] These goals translate into enduring themes for the military: (1) Protect the Party and Safeguard Stability, (2) Defend Sovereignty and Defeat Aggression, (3) Modernize the Military and Build the Nation.[82] To accomplish these ends, the MND assigns its armed forces strategic tasks *(zhanlüe renwu),* which guide the employment of resources to accomplish objectives.

Clearly defining a credible cyber deterrent is quite difficult when norms of cyber behavior remain ill-defined.

Both US and China militaries design strategy to support national policy goals. When outlining and designing strategy, the US military often uses an ends-ways-means heuristic.[83] The US military derives strategic guidance from national leaders and then develops the ways and means to accomplish those *ends.*[84] The PLA shares a similar affinity for designing strategy subordinate to national policy.[85] PLA theater strategy likewise implements national strategy.[86] This paper uses an ends-ways-mean framework to simplify and summarize PLA strategic thinking for an American audience.

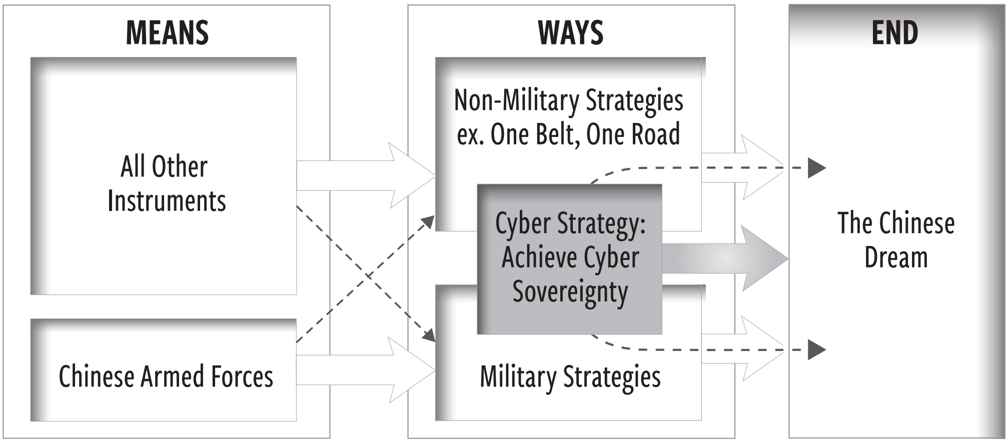


Figure 1: A simplified outline of China's national strategy

In the standard narrative, as China pursues the Chinese Dream, its strategy must meet two decisive milestones called the "two centenaries" *(liang ge yibai nian).*[87] The first centenary occurs in 2021, one hundred years after the CCP's establishment. At that time, China expects to become a moderately prosperous society.[88] The second centenary in 2049 marks one hundred years since the Communists won China's civil war. By this point, China plans to consolidate a "prosperous, strong, democratic, culturally advanced and harmonious" society.[89] In October 2015, the Fifth Plenary Session of the 18th CCP Central Committee reaffirmed the two centenaries in its 13th Five-Year Plan.[90] In an address to the United Nations, Xi identified international stability as one necessary condition for the Chinese Dream.[91] Xi evaluates foreign and domestic policy in terms of achieving the Chinese Dream in step with the two centenaries.[92] Thus, the Chinese Dream and the two centenaries orient and pace the PLA as it operationalizes the national military strategy.

In the cyber domain, leaders have unique *ways* and *means* to pursue objectives. For example, Lieutenant General (retired) Wang Hongguang believes cyber operations enable China to achieve reunification with Taiwan and realize the Chinese Dream without lethal military conflict.[93] The general, a standing committee member of the 12th National Committee of the Chinese People's Political Consultative Conference (CPPCC), argues the PLA must develop sophisticated cyber capabilities to "defeat its adversaries without fighting" *(bu zhan er qu ren zhi bing).*[94] General Wang, a former deputy commander of the Nanjing Military Region, sees cyber capabilities as an asymmetric response to the superior military power of the US and Japan. [95] The general conveys just one of many ways the PLA can leverage cyber operations to achieve strategic *ends.*

Cyber sovereignty: a way to reach the Chinese Dream

To achieve the Chinese Dream, the CCP believes it must secure sovereignty in cyberspace. In 2007, then-President Hu Jintao told Party leaders, "Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state."[96] Beijing requires internal stability and insulation from external threats to realize the Chinese Dream, and these twin imperatives extend to cyberspace. For example, Lieutenant General Wang Xixin calls for the PLA to employ cyber forces to win future conflicts under the conditions of informationized warfare (xinxihua tiaojian xia kongzhi zhan). [97] In this way, the PLA field's cyber forces to accomplish missions in the information environment, which in turn ensures the CCP achieves cyber sovereignty.

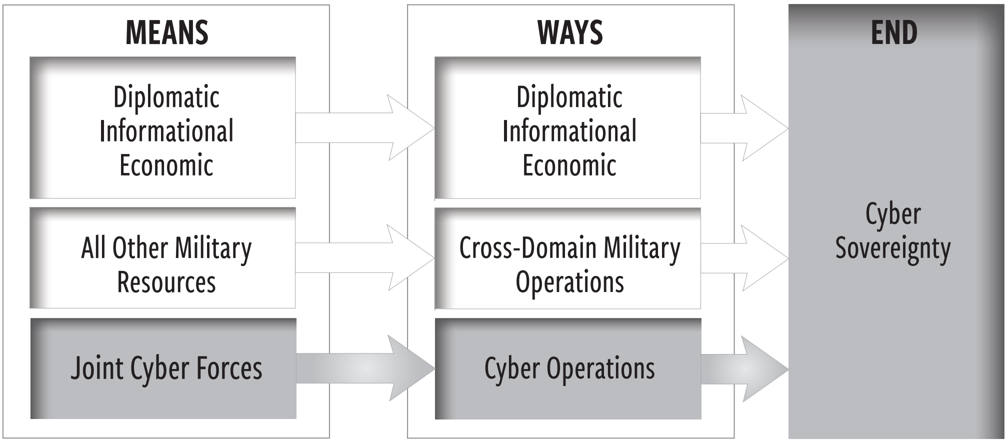


Figure 2: Simplified outline of China's cyber strategy

In 2011, China's pursuit of cyber sovereignty collided with US policy when the White House published its *International Strategy for Cyberspace.* This US policy document promoted an approach to global cybersecurity in accordance with America's "core commitments to fundamental freedoms, privacy, and the free flow of information." [98] China's officials criticized the strategy as a veiled justification for US hegemony in cyberspace. [99] In their analysis, PLA Senior Colonel Ye Zheng and Captain Zhao Baoxian predict the US will pursue cybersecurity with the same self-interest seen in economic and military affairs. Furthermore, the PLA officers expect the US to launch cyber operations whenever necessary to protect its networks *(wuli huwang).* After the Stuxnet attack on Iran's centrifuges, Colonel Ye and Captain Zhao concluded even China's physically isolated networks remain vulnerable to US cyber-attack; passive cyber defense alone is insufficient. Therefore, China must achieve parity with the US in cyberspace to deter aggression and protect national sovereignty. [100]

The 2015 *Military Strategy* affirms the PLA mission to "safeguard China's sovereignty, security and development interests, and provide a strong guarantee for achieving the national strategic goal of the 'two centenaries' and for realizing the Chinese Dream."[101] In the current and future information environment, China considers cyberspace the "new commanding heights in strategic competition" among advanced countries.[102] Although public literature does not offer a stand-alone PLA cyber strategy document, various texts can be summarized through the ends-ways-means framework.[103]

FIGURE 3: THE ENDS-WAYS-MEANS OF CHINA'S CYBER STRATEGY

Ends: Cyber sovereignty; the CCP retains authority in cyberspace and safeguards the Chinese Dream across all domains; China exercises full sovereignty across all domains

Ways:

- Stop and control major cyber crises (e kong wangluo kongjian zhongda weiji)
- Protect national network and information security (baozhang guojia wangluo yu xinxi anquan)
- Safeguard national security and social stability (weihu guojia anquan he shehui wending)
- Support the country's endeavors in cyberspace (zhiyuan guojia wangluo kongjian douzheng)
- Participate in international cyber cooperation (canyu guojia hezuo)

Means: A new joint cyber force (wangluo kongjian liliang jianshe) with the following advanced cyber capabilities:

- Cyber situational understanding (wangluo kongjian taishi ganzhi)
- Cyber defense (kongjian fangyu)
- Precise targeting (jingda quebao weishe)

Major General Chen Zhou explains cyberspace imperatives require China to accelerate cyber situational awareness, cyber defense, the ability to compete in cyberspace, and the ability to collaborate with the international community. With these *means*, China will be able to safeguard national cybersecurity and information security.[104] Similarly, the 2015 *Military Strategy* directs the armed forces to develop the requisite cyber *means* to accomplish assigned tasks. Given this guidance, the PLA must develop doctrine to guide the development and employment of joint cyber forces.

PART 3: US CYBER DETERRENCE

The military doctrine that guides cyber operations has evolved along with cyber capabilities. Do previous paradigms apply in the virtual world? Military theories of airpower and seapower offer one starting point.[105] Nuclear deterrence theory appears helpful in evaluating the interplay of actors armed with devastating weapons.[106] In 2006, the Pentagon endorsed deterrence as a way to dissuade potential adversaries in cyberspace.[107] In December 2015, the White House circulated its cyber deterrence strategy, declaring the US would use "all instruments of national power to deter cyber-attacks or other malicious cyber activity that pose a significant threat to the national or economic security of the United States or its vital interests."[108] The US and China are militarily and economically dependent on cyberspace, and such dependency seemingly guarantees successful mutual deterrence.[109] Yet, deterrence does not dissuade all adversaries,[110] and current US cyber deterrence strategy appears poorly calibrated for deterring China, a resolute and increasingly sophisticated actor in cyberspace.

In many ways, cyber operations and electromagnetic warfare represent quintessential asymmetric threats. Unlike conventional and nuclear weapons, cyber capabilities provide adversaries low-cost military power that targets the vulnerabilities of America's information economy. New America Foundation's P.W. Singer warns, "The problem is that the evidence disproves this link between building up more cyber-offensive capability as the way to scare off the other side. There is not yet any direct pathway to deterrence the way building up nuclear capability yielded it back in the day."[111] If mutual deterrence does not fully translate to cyberspace, the international community must at minimum develop norms that delineate proper cyber behavior.[112] Graham Webster, a Senior Fellow of the Paul Tsai China Center at Yale Law School, writes, "Not every 'cyber' incident is created equal, and retaliation without a clearly communicated principle simply wouldn't deter anything in particular."[113] Clearly established redlines between cyber espionage and cyber warfare, for example, can help reduce the likelihood of unintended escalation.[114]

> Recent US-China interactions in the South China Sea have exemplified the potential for mishap under the compellent form of weishe.

To its credit, the White House appears to appreciate these nuances, and its cyber deterrence strategy seeks international consensus on the "appropriate responses for cyberattacks."[115] President Obama even pushed for an agreement on cyberspace norms at the 2015 G20 summit.[116] This cooperative mindset does not preclude developing" improved defenses, more resilient architectures, and a range of options–cyber and non-cyber—to inflict costs and to hold accountable adversaries that choose to conduct cyberattacks or other malicious activity against U.S. interests."[117] The measured tone of the US cyber deterrence strategy appears to recognize the inherent limits of extending traditional deterrence into the cyber domain.

Nevertheless, the US cyber deterrence strategy has attracted sharp critiques within the US government. Senator John McCain, Chairman of the Senate Armed Services Committee, criticized the White House for failing "to integrate ends, ways and means to meaningfully deter attacks in cyber space."[118] He chastised the report for going "to great pains to minimize the role of offensive cyber capabilities and doing little to clarify the policy ambiguities that undermine the credibility of deterrence."[119] Notwithstanding this feedback, clearly defining a credible cyber deterrent is quite difficult when norms of cyber behavior remain ill-defined.

This high-stakes provocation follows a military weishe approach and reveals a PLA mindset that optimistically assumes American restraint.

Defining deterrence

Military deterrence has long been a pillar of US national security policy in assorted forms across various domains. Yet, such an enduring concept remains ill-defined within US-China relations because the two countries conceptualize deterrence differently. The Pentagon defines deterrence as "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."[120] Meanwhile, China embeds deterrence within a broader concept of *weishe* that combines deterrence and compellence.[121] In the West, military art distinguishes between deterrence and compellence,[122] but many PLA texts operationalize military *weishe* without clear distinctions between the twin concepts. Even in peacetime, PLA commanders appear to view certain compellent actions as legitimate, while the US and its allies consider them offensive operations.

Western military literature predominantly translates *weishe* as deterrence, but the concept is better interpreted as a particular form of coercion. In his 1966 *Arms and Influence,* Thomas Schelling defined coercion in two parts, deterrence and compellence, and dissected those terms:

> Deterrence and compellence differ in a number of respects, most of them corresponding to something like the difference between statics and dynamics. Deterrence involves setting the stage—by announcement, by rigging the trip-wire,

> by incurring the obligation—and *waiting*. The overt act is up to the opponent. The stage-setting can often be nonintrusive, nonhostile, nonprovocative. The act that is intrusive, hostile, or provocative is usually the one to be deterred; the deterrent threat only changes the consequences *if* the act in question—the one to be deterred—is then taken. Compellence, in contrast, usually involves *initiating* an action (or an irrevocable commitment to action) that can cease, or become harmless, only if the opponent responds. The overt act, the first step, is up to the side that makes a compellent threat. To deter, one digs in, or lays a minefield, and waits—in the interest of inaction. To compel, one gets up enough momentum (figuratively, but sometimes literally) to make the other *act* to avoid collision … Compellence has to be definite: We move, and you must get out of the way.[123]

China appears willing to employ provocative measures to compel a change in US policy and secure its interests in the region.

China's Research Department of Military Strategy defines military *weishe* as a "strategic operation, with the threat to use or the actual use of military capability in order to influence the adversary's strategic judgments by making the adversary feel [that it is too] difficult to achieve anticipated targets or the cost may exceed the benefit."[124] The "actual use of military capability" suggests a broad spectrum of military activities. From benign to dangerous, *weishe* actions increase uncertainty and risk escalation. If Beijing orders military action to compel Washington to change a policy, the operation may unintentionally cross an American redline that then escalates an otherwise manageable dispute.

Recent US-China interactions in the South China Sea have exemplified the potential for mishap under the compellent form of *weishe.* Beijing seeks unchallenged authority over its maritime claims and treats the South China Sea as an issue of sovereignty. Meanwhile, the US Navy operates freely in international waters according to established norms. China interprets US naval operations as a challenge to its national security. In 2009, Chinese white-hulled vessels aggressively maneuvered against the USNS *Impeccable* and nearly caused a collision. In this instance, Beijing used non-military coercion and chanced military conflict to compel a shift in US policy.[125] This high-stakes provocation follows a military *weishe* approach and reveals a PLA mindset that optimistically assumes American restraint.

Numerous PLA theorists have written about warfare in the twenty-first century. Regarding *weishe,* prevailing thought appears to hold "a country should not hesitate to deter through military force if there is no other way to control a crisis."[126] At times, China's deterrence parallels US notions. For example, the PLA expects its state-of-the-art air power to "discourage other countries from conducting air and other military operations against China or to convince any adversary to abandon its own military operations."[127] Yet, the compellence form of *weishe* still resembles US offensive operations. For example, China considers space weapons that target satellites a form of *weishe* at the extreme end of the peacetime continuum, but the US treats such weapons as offensive capabilities for war.[128] This incongruence between US deterrence and China's *weishe* degrades escalation management by fomenting miscues. This US-China doctrinal gap is especially relevant to cyber operations given persistent ambiguity about appropriate behavior in cyberspace.

Although publications often translate *weishe* as deterrence, such expediency encourages an erroneous frame for Chinese actions. This paper therefore retains the term *weishe* when discussing Chinese texts to aid accurate interpretation of Chinese signaling. Summarizing China doctrine, Kevin Pollpeter of UC San Diego's Institute on Global Conflict and Cooperation (IGCC) explains, "Effective coercion [*weishe*] not only requires a strong capability and the will to carry out threats, those threats must be communicated effectively so that the target of the coercion is cognizant of the full costs of coming into conflict with China."[129] The emphasis on signaling requires Washington to understand Beijing's message. Therefore, China must calibrate its message for its intended audience before launching an irrevocable course-of-action. Ultimately, peace between the US and China rests on maturity and mutual understanding.

One unofficial cyber weishe approach

The PLA considers compellent forms of *weishe* legitimate in peacetime. Extending *weishe* to cyberspace meanwhile remains a nascent concept. AMS researcher Yuan Yi proposes one approach for cyber *weishe*. Yuan believes cyberspace is a strategic area with *weishe* opportunities.[130] In the twenty-first century, he argues the PLA must employ cyber operations to achieve *weishe* across all domains. According to Yuan's cyber *weishe* approach, cyber operations must showcase an adversary's impotence in the physical and virtual worlds.[131]

FIGURE 4: YUAN YI'S REQUIREMENTS FOR EFFECTIVE CYBER WEISHE

Build the proper cyber force: Well-organized joint cyber force *(wangluo zhan liliang xingcheng heli)* that can organize and coordinate the power of the network of 'patriotic' hackers *(aiguo heike).*

Select the proper target: Must identify high-value targets that clearly demonstrate China's role because an innocuous attack could be incorrectly attributed to common hackers *(yi bei wu renwei shi putong heike zhizao)* and fail to achieve the desired effect of deterrence. Cyber operations require sophisticated precision *(jing da quebao weishe)* to prove the futility of challenging Chinese interests.

Execute information campaign: Before attack, China must issue a warning to the adversary through extensive propaganda *(yao tongguo guangfan de yunlan xuanchuan zaoshi, xiang diguo fachu daji jinggao).* After attack, ensure adversary recognizes China's superb cyber capabilities *(yi zhanxian jifang gaochao de wangluo gongji jishu he shoudian).*

Yuan's cyber *weishe* approach exceeds the scope of deterrence under US doctrine. Yuan even concedes dangerous uncertainty in his cyber *weishe* proposal because he cannot predict US reactions to aggressive cyber operations.[132] In 2014, Yuan coauthored a piece in a PLA newspaper that rebuked US cyberspace hegemony and called for the mobilization of Chinese citizens to carry out massive cyber-attacks against the US.[133] Yuan presents a highly aggressive perspective in PLA cyberspace thinking. Commenting on Yuan's proposal, CFR's Adam Segal writes, "The article is almost definitely not an authoritative overview of what the People's Liberation Army thinks about deterrence but at the same time it is equally unlikely to be completely outside the mainstream."[134] To marginalize Yuan-like thinking, Segal hopes leaders from both countries will "meet soon, and start the discussion on the meaning of deterrence and other basic concepts."[135] Segal's concerns seem prudent given the risks of escalation a Yuan-like mindset imbues.

A cyber weishe interpretation of the 2014 OPM cybersecurity breach

Prior to the Obama-Xi summit in September 2015, one of the most discussed national cybersecurity topics was the 2014 breach at the US Office of Personnel Management (OPM).[136] Most likely a PLA cyber operation, the OPM breach exposed the sensitive information of nearly 22 million current and former government personnel, contractors, and family members. The impact of the OPM breach continues to reverberate. On February 22, 2016, OPM's chief information officer resigned over the scandal seven months after the OPM's director also departed.[137] In September 2015, the CIA reported the OPM hack forced the Agency to withdraw compromised intelligence officers from the field.[138] US officials described the OPM breach as cyber espionage, and most media coverage cited the intelligence value of the stolen information as an explanation for the breach. The China's government claims the OPM breach was a cybercrime, not state-sponsored espionage.[139] and they even arrested several alleged hackers.[140] Nevertheless, the US intelligence community remains confident the breach was a state-sanctioned cyber operation. By characterizing the event as cyber espionage, the US deemed the breach a case of spying that all governments conduct during peacetime.

Although cyber espionage offers a reasonable explanation for the OPM breach, this paper offers an alternative interpretation. Rather than a matter of spying, the OPM breach appears to be a categorical success under cyber *weishe*. The cyberattack struck a high-value target with very little collateral damage, showcased the sophistication of Chinese cyber forces, compelled US leaders to revisit cybersecurity policies, and signaled

China's willingness to use cyber operations for national security ends. In accordance with military *weishe*, the cyberattack selected a target that generated a tolerable US response. Despite public scrutiny and embarrassment, the Obama administration remained considerably restrained. Admiral Mike Rogers told the Atlantic Council that the OPM breach was part of a significant PLA information collection effort.[141] Director of National Intelligence James Clapper identified China as the likely culprit, but the administration did not escalate rhetoric much further.[142] General (retired) Michael Hayden, former head of the NSA and the CIA, assessed OPM's repository as a legitimate target for cyber espionage.[143] By choosing cyber espionage as opposed to a Stuxnet-like attack, China's leaders astutely kept their cyber operation within the scope of acceptable peacetime activities.

Around the world, emerging military powers are building capabilities that intentionally enhance uncertainty.

The purpose for the OPM breach can be interpreted through the lens of China's cyber strategy, which pursues cyber sovereignty. Thus, the Obama-Xi summit can be seen as a victory for China's cyber sovereignty agenda: two presidents directly discussing a state's duty to govern its citizens and enforce laws in cyberspace. President Obama delivered stern remarks about the need for China's government to curb cybercrime, but the OPM breach did not feature in public discussions.[144] The two presidents agreed that stealing intellectual property undermines the international economic order.[145] In accordance with cyber *weishe*, PLA cyber operations compelled Washington to elevate cybersecurity to the highest levels of diplomacy and partially validate China's arguments for sovereign control in cyberspace governance.

After the Obama-Xi summit, the US intelligence community assessed that PLA cyber operations would continue apace.[146] Xi escaped overt criticism while advancing China's cyberspace agenda. Beijing leveraged the summit to promote its view that only national governments can effectively secure cyberspace. In this way, the OPM breach may have helped compel Washington to partially acquiesce to Beijing's pursuit of cyber sovereignty. In December 2015, US and China envoys launched the cybersecurity dialogue agreed upon during the Obama-Xi summit. Meanwhile, Xi addressed the World Internet Conference and strongly advocated for cyber sovereignty as the future paradigm for Internet governance.[147] Clearly, China continues to pursue cyber sovereignty.

Harvard's Jack Goldsmith also believes Xi used US reaction to China's cybercrime for domestic purposes. Goldsmith points to a precipitous drop in commercial cyber espionage well before the presidential summit in September 2015.[148] Goldsmith interprets changes in Chinese cyber behavior as "less about the U.S. imposing or threatening hefty costs on a unitary China (the costs and threatened costs have not in fact been hefty), and more about the U.S. making transparent corrupt state-sponsored activities to China's government, and thus aiding China's government (as embodied in Xi's regime) in furthering its interests."[149] In this view, the 2015 presidential summit helped Xi consolidate control over cyberspace within China.

In short, cyber operations like the OPM breach should be assessed beyond their intelligence value. When PLA cyber operations are controlled at the highest echelons, such activities merit thorough analysis of second- and third-order effects. This paper argues such cyberattacks aim to compel the US to react in ways that erode the sanctity of an open Internet. If the strategic objective of China's cyber strategy is cyber sovereignty, then the US remains the largest obstacle to China's ambitions to displace the status quo. Thus, in accordance with cyber *weishe*, Beijing will act to undermine multistakeholder cyberspace governance, compel Washington to acquiesce to cyber sovereignty, and galvanize international support for rewriting norms that govern the Internet.

PART 4: DOCTRINAL DIFFERENCES BETWEEN US AND CHINA

Just as the US and China diverge on their understanding of deterrence, the military doctrine of the two countries further aggravates misunderstandings over cyber operations. China expert Gregory Kulacki notes, "PLA strategy is focused on understanding and responding to U.S. investments in the advanced conventional military capabilities it believes the United States intends to use to undermine the credibility of China's overall military deterrent."[150] Consequently, the US-China military relations suffer a feedback loop where the strategic decisions of one country influence the decisions of the other. As US and China strategists estimate the future actions of one another, miscalculation appears inevitable.

As mentioned previously, the South China Sea illustrates opportunities for such misunderstandings. The Naval War College's Peter Dutton argues the "combination of economic leverage, civilian maritime power, and military deterrence power has enabled a Chinese strategy in which there are little or no consequences for the employment of escalation, short of militarized armed conflict.".[151] Dutton identifies a gap between US and China doctrine in which China employs "non-militarized coercion" to achieve strategic objectives.[152] According to Dutton, recent maritime patrols exemplify China's predilection for non-militarized coercion. China's white-hulled vessels outnumber the combined maritime forces (navy and coast guard) of all other South East Asian neighbors. China now exercises "de facto control over much of the disputed water space."[153] From the US perspective, such activities destabilize regional stability, but China's actions align with its tradition of military *weishe*. China appears willing to employ provocative measures to compel a change in US policy and secure its interests in the region.

As cyber capabilities evolve on both sides of the Pacific, US and China cyber operations will intensify the consequences of warfare in the twenty-first century information environment.[154] University of Toronto's Jon Lindsay warns, "The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution." [155] Lindsay also writes, "Overlap across political, intelligence, military, and institutional threat narratives makes cybersecurity a challenging policy problem, which can lead to theoretical confusion." [156] In this way, doctrinal confusion can generate misunderstandings with serious consequences.

Doctrine-difference theory

To explore the consequences of doctrinal confusion, Naval Postgraduate School's Christopher Twomey tests "the causal claim that doctrinal differences worsen misperceptions, which can lead to escalation."[157] In one case, he applies doctrinal-difference theory to China's decision to escalate involvement in the Korean War after American-led forces crossed the 38th parallel in October 1950. America's aggressive pursuit of North Korean forces stoked Chinese fears about an anti-communist bloc in Northeast Asia. [158] Beijing could not tolerate a unified anti-communist Korea. By November, tens of thousands of PLA soldiers had entered combat in North Korea. In hindsight Beijing had strongly signaled their interests on the Korean Peninsula well before it entered the war; however, the US failed to recognize the gravity of China's redlines. [159]

On September 7, 1950, the National Security Council concluded, "Although politically unlikely, it is possible that Chinese Communist forces might be used to occupy North Korea … it is possible that the Soviet Union, although this would increase the chance of general war, may endeavor to persuade the Chinese Communists to enter the Korean campaign." [160] On October 2, the White House authorized General Douglas MacArthur to operate north of the 38th parallel. In months preceding this decision, the PLA had visibly prepared for a Korean contingency. During the summer of 1950, Mao Zedong redeployed troops to Manchuria from their Taiwan-invasion posture in Fujian. For several weeks, PLA infantry formations conducted exercises near the Korean border, signaling China's intent to check a US maneuver northward. On the diplomatic front, strategic dialogue proved wholly insufficient, because Beijing and Washington had not restored diplomatic relations following China's civil war. [161] The two countries failed to retain a mechanism for mitigating tensions or preventing escalation.

Meanwhile, MacArthur and his staff misinterpreted PLA doctrine and underestimated Beijing's commitment to the Korean Peninsula. The US military erroneously assumed its air power would neutralize the PLA. Moreover, MacArthur expected China to commit their main effort near the 38th parallel as the Americans maneuvered across the mountainous terrain. [162] In fact, the main PLA forces were postured much further north. PLA doctrine dictated a "lure them in deep" operational approach that encouraged American forces to extend their supply lines into North Korea's restrictive terrain. [163] As late as December, the US continued to grossly underestimate the massive number of PLA troops it faced. [164]

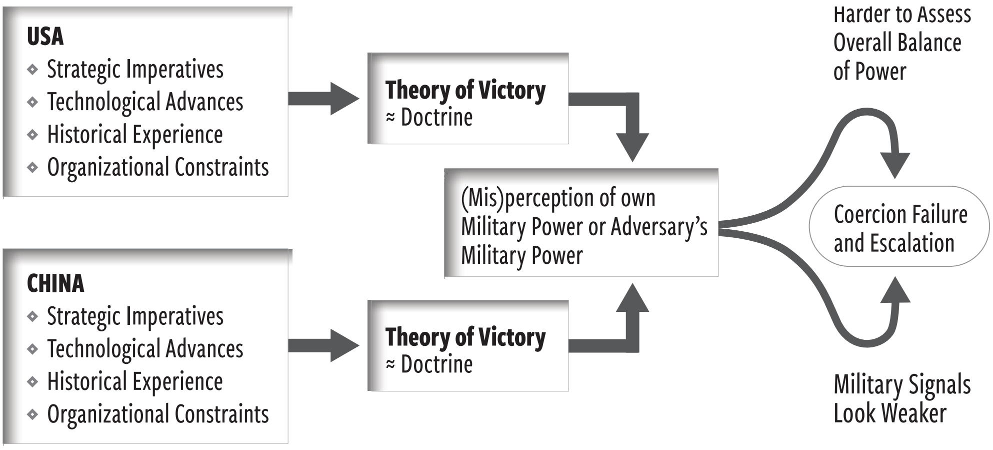

USA
Strategic Imperatives
Technological Advances
Historical Experience
Organizational Constraints
CHINA
Strategic Imperatives
Technological Advances
Historical Experience
Organizational Constraints
Theory of Victory
≈ Doctrine
Theory of Victory
≈ Doctrine
(Mis)perception of own Military Power or Adversary's Military Power
Harder to Assess Overall Balance of Power
Coercion Failure and Escalation
Military Signals Look Weaker

Figure 3: Modified Twomey Doctrinal-Difference Model

The US-China confrontation in the Korean War illustrates "the link between different theories of victory and underestimation of the enemy." [165] Twomey explains, "Differences in theories of victory here directly contributed to U.S. misperception of its adversary's relative capabilities. This suggests that American assessments of the balance of power and of Chinese signals before the war were adversely affected by the misperceptions.". [166] Although the US intelligence assets observed PLA exercises in Manchuria, Washington did not interpret the signals as commitment to intervention. Additionally, MacArthur underestimated the PLA's strength and capabilities. [167] The deterrence aspect of *weishe* failed for China. The divergence between Chinese and American military thinking intensified a war that killed over 36,000 Americans, 1.2 million South Koreans, a million North Koreans, and 600,000 Chinese troops. [168]

Accurately interpreting an adversary's doctrine is necessary for predicting its actions in a deterrence approach. Since *weishe* relies on signaling, misperception of military signals increases the likelihood of a weishe failure and unintended escalation. In 2000, George Washington University's David Shambaugh called PLA doctrine the driving force behind "all other facets of China's military modernization." [169] Hence, the US must accurately understand PLA military theory to ensure national security. Doctrine reveals a military's approach to tactical, operational and strategic decisions; it is the key to deciphering military signals.

PLA doctrine is subordinate to national strategic interests and guides the military's transformation. [170] Similarly, the US military treats doctrine as the foundation for military training and operations. [171] Unlike the US military, the PLA integrate political thought into military decision-making at all echelons. [172] These political imperatives shape training, operations, and strategic design within the PLA. In addition, the PLA operate with a far more asymmetric mindset than the US military. [173] PLA and US military doctrine differs, which shapes their respective military strategy and operations. [174]

Across all domains, accurately evaluating an adversary’s doctrine remains fraught with challenges. In cyberspace, the intent behind military activity appears even more obscure. Such uncertainty regarding the purpose of an adversary’s cyber operations muddles the taxonomy of threats and undermines the effectiveness of a cyber deterrent.[175] Doctrinal-difference theory warns that today’s cybersecurity status quo carries serious risks of doctrinal confusion, coercion failure, and escalation.

A growing military affinity for ambiguity

To prevent unintended war, strategists traditionally reduce ambiguity. Yet, around the world, emerging military powers are building capabilities that intentionally enhance uncertainty. In 2015, US Joint Chiefs of Staff described a new hybrid threat, which “blends conventional and irregular forces to create ambiguity, seize the initiative, and paralyze the adversary.”[176] Hybrid conflicts “increase ambiguity, complicate decision-making, and slow the coordination of effective responses.”[177] The US military believes future adversaries are pursuing asymmetric capacity for hybrid warfare.[178] The U.S. Army operates under the assumption that “changes in technology and geopolitical dynamics as well as the enduring political and human nature of war will keep war in the realms of complexity and uncertainty.”[179] In response to this threat, the US military is investing in technologies and organizational structures that boost agility to respond to unpredictable threats.[180] The US finds it increasingly difficult to prepare for future conflicts.

The US must clearly delineate redlines for cyberspace behavior to prevent PLA cyber operations from unnecessarily provoking a conflict.

PLA military theorists have reached a similar conclusion about twenty-first century warfare. Lieutenant General Wang Xixin predicts China faces an era of low-intensity conflict requiring new operational approaches.[181] The PLA fears “conflict may erupt from a crisis that has spiraled out of control, rather than from an intent to start a war.”[182]] PLA Colonel Lin Dong argues China’s military thinking remains underprepared for future threats. Interestingly, he also believes the US military practices a form of hybrid warfare (*hunhe zhanzheng*), and the PLA must therefore adopt a new political-military theory that better integrates military strategy with foreign policy.[183] Like the US military, the PLA sees an era of uncertainty that requires careful management to minimize the scale of future crises.

Unfortunately, this era of uncertainty extends to cyberspace. The divergent views of cyber deterrence and cyber *weishe* seem ripe for future conflict. Adam Segal writes, “Beijing and Washington have a common interest in preventing escalatory cyber operations–attacks that one side sees as legitimate surveillance but the other views as prepping the battlefield.”[184] Segal recommends, “The two sides could consider conducting formal discussions on acceptable norms of behavior and possible thresholds for use of force as well as greater transparency on doctrine. These cooperative measures can reduce the chance of misperception and miscalculation and thus diminish the likelihood that a conflict in cyberspace will become kinetic."[185] In a security environment wrought with uncertainty, two great powers can ill-afford misinterpretations.

The search for mutual understanding

For years, mutual understanding has been the hallmark of international cyber policy. On December 29, 2009, the United Nations General Assembly adopted a resolution affirming the necessity of cooperation for global cybersecurity.[186] At a 2012 conference with his Chinese counterpart, Secretary of Defense Leon Panetta emphasized the importance of working "together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area [of cyber defense]."[187] In 2015, US State Department's Michele Markoff emphasized mutual understanding during a panel discussion in Beijing. As the deputy director of the Office of the Coordinator for Cyber Affairs, Markoff encouraged countries to develop "practical cyber confidence building measures" and promote international norms in cyberspace.[188]

Despite espousing mutual understanding, US-China mistrust over cybersecurity remains pervasive. In July 2014, Secretary of State John Kerry and State Councilor Yang Jiechi met in Beijing at the sixth round of the US-China Strategic and Economic Dialogue (S&ED). Among a long list of topics, the strategic dialogue reaffirmed an imperative to "build greater mutual understanding in military-to-military relations through improved communication and contacts at all levels."[189] Reflecting on the S&ED, senior Chinese diplomat Zhou Jingxing assessed, "the insufficiency of strategic mutual trust is the root of all problems between the US and China."[190] Senior Colonel Zhao Zijin and Colonel Zhao Jingfang argue military crises often occur by accident, but the root causes (*baofa genyuan*) are fundamental conflicts of interest between countries and political groups. So long as disputes remain unresolved, they argue, unfortunate incidents can escalate into crises.

Even if disputes remain unresolved, the US and China can still develop mechanisms to deescalate situations. Former assistant secretary of state for East Asian and Pacific affairs Kurt Campbell states, "It is probably inevitable that there is going to be more tension in the relationship between the United States and China going forward. So, learning how to deal with that tension and manage it effectively will be one of our great challenges."[191] Similarly, US Army Brigadier General Kimberly Field and Major Stephan Pikner predict that US-China relations will encounter "points of friction, especially given America's (admittedly intermittent) underwriting of the Responsibility to Protect doctrine that contrasts starkly with China's emphasis on state sovereignty as paramount."[192] The two Army officers advocate "a framework of mutual restraint between the United States and China, in conjunction with a broader engagement strategy."[193] Both Field and Pikner hope to avoid accidental escalation through increased collaboration.

Lauding the September summit, Obama stated, "The candid conversations between President Xi and myself about areas of disagreement help us to understand each other better, to avoid misunderstandings or miscalculations, and pave the way potentially for further progress in those areas."[194] Xi said the two countries must enhance strategic trust, increase mutual understanding, and respect each country's interests. China's president emphasized US-China relations face a single option: win-win cooperation.[195] Despite the proclaimed goal of mutual understanding in cyberspace, the summit produced modest outcomes. [196] Trust remains an aspiration.

Four Recommendations

Ultimately, the goal of US cyber deterrence is to prevent cyberattacks, and current US cyber policy likely deters many threats. With respect to China, the US must clearly delineate redlines for cyberspace behavior to prevent PLA cyber operations from unnecessarily provoking a conflict. The four following recommendation are meant to help promote this goal.

1. **Continue the cybersecurity dialogue:** The Obama-Xi summit directed experts to improve mutual understanding over cybersecurity. These meetings are conduits for developing confidence-building measures and could eventually design mechanisms to deescalate future cyber-related crises. When cyberattacks and retaliation move at light speed, decision-makers must carefully manage escalation.

2. **Produce a Glossary of Cybersecurity Terms:** Written in English and Chinese, experts should produce a comprehensive document that clarifies each government's official stance on cyber operations. The details of this publication should mirror the *United States-Chinese Glossary of Nuclear Security Terms* by the Committee on International Security and Arms Control (CISAC) of the American National Academies of Science (NAS). The cybersecurity working group should produce doctrinal definitions that Chinese and English linguists absolutely concur reflect the intent of both governments. As US-China teams collaborate, they should especially dissect each government's view of cyber deterrence. This challenging exercise could eventually help construct inclusive global norms for cyberspace behavior, which could then boost cybersecurity for all stakeholders worldwide.

3. **Encourage Track 1.5/2 diplomacy addressing cyber deterrence:** Diplomatic channels facilitate valuable dialogue. Current and former US policymakers should meet with their Chinese counterparts to discuss cyber deterrence at various forums like the Shangri-La Dialogue and the U.S. Strategic Command (USSTRATCOM) Deterrence Symposium. US organizations like the Carnegie-Tsinghua Center should invite American and Chinese experts to conferences that address cyber deterrence.

4. **Commission a study of Chinese cyber deterrence for public release:** The Department of Defense should commission an organization like RAND or CNA to produce a report summarizing PLA military thinking on cyber deterrence. The final report should be made public to entice Beijing to critique the interpretation of China cyber policy. CSIS, Brookings, or other think tanks should then invite China's leaders to speak at events and debate the merits of this semi-official report. Through these channels, China officials will feel compelled to clarify ambiguous cyber policies.

These four recommendations require US officials and their partners to sufficiently understand US cyber policy. Specifically, the US must clearly articulate redlines so that current and former officials can accurately convey them to Chinese counterparts. Furthermore, this paper's recommendations rely on Beijing's reciprocity in clarifying their doctrine.

Given the complexity of evolving US cyber policy, interagency cooperation may need to produce a primer that summarizes US cyber policy. Developing interagency consensus such a document offers an opportunity to clarify the ends-ways-means of US strategic thinking on cyberspace. Perhaps this exercise would help identify and rectify inconsistencies across various US agencies and promote unity of effort in cyber defense.

As Beijing pursues cyber sovereignty, it appears willing to use cyber operations to compel the US to reorient its cyber policy. The US cyber deterrence strategy rightly promotes international cooperation, public-private partnerships, multi-stakeholder governance, and critical infrastructure protection. On the other hand, the cyber deterrence strategy also intentionally promotes "uncertainty in adversaries' minds about the effectiveness of any malicious cyber activities and to increase the costs and consequences that adversaries face as a result of their actions."[197] Deliberately boosting ambiguity may prove effective against most adversaries, but it seems counterproductive when trying to deter an assertive China. Thus, US military commanders, their staffs, and policymakers require an appreciation for the nuances of China's views on cyber operations. As a sophisticated actor in cyberspace, China warrants a sophisticated cyber defense policy that appreciates its particularities.

Today, doctrinal confusion in the cyber domain appears untenable. The US-supported multi-stakeholder approach to Internet governance has failed to persuade many governments that seem apt to support Beijing and Moscow. If an open Internet is a US strategic interest, the erosion of multi-stakeholder governance should alarm strategists. In today's information environment, China continues to pursue cyber sovereignty, which fundamentally clashes with America's vision. As these two great powers pursue incompatible strategic objectives in cyberspace, their ambitions seem ripe for confrontation. To prevent such disputes from accidently spiraling out of control, Beijing and Washington must clarify their doctrinal differences and develop mechanism for de-escalation to avoid the calamity of a cyber war.

NOTES

[1] “Chinese military launches two new wings for space and cyber age,” *South China Morning Post*, January 1, 2016, accessed January 3, 2016, http://www.scmp.com/news/china/diplomacy-defence/article/1897356/chinese-military-launches-two-new-wings-space-and-cyber.

[2] “China: The Power of Military Organization,” *Stratfor,* January 25, 2016, accessed March 12, 2016, https://www.stratfor.com/analysis/china-power-military-organization.

[3] David M. Finkelstein, “Initial Thoughts on the Reorganization and Reform of the PLA,” *CNA Occasional Paper* (January 15, 2016), 2.

[4] Zhang Jianfeng, ed., “China inaugurates PLA Rocket Force as military reform deepens,” *Xinhua*, January 2, 2016.

[5] John Costello, “The Strategic Support Force: China’s Information Warfare Service,” *China Brief* 16, No. 3 (February 8, 2016), accessed March 12, 2016, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45075&no_cache=1#.VubSypMrJE4.

[6] “Expert: PLA Strategic Support Force a key force to win wars,” *China Military Online*, January 6, 2016, accessed January 7, 2016, http://eng.mod.gov.cn/TopNews/2016-01/06/content_4635472.htm.

[7] Wu Gang, “China upgrades missile force, adds space and cyber war forces,” *Global Times*, January 1, 2016, accessed January 9, 2016, http://www.globaltimes.cn/content/961440.shtml.

[8] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” *Project 2049 Institute* (November 11, 2011), 7.

[9] Lü Jinghua [吕晶华], “Gongtong goujian heping anquan kaifang hezuo de wangluo kongjian,” [共同构建和平安全开放合作的网络空间] (Jointly building a peaceful and safe cyberspace through open cooperation) *PLA Daily,* October 18, 2016, http://www.81.cn/jfjbmap/content/2015-10/18/content_126334.htm.

[10] Stuart N. Brotman, “Multistakeholder Internet governance: A pathway completed, the road ahead,” *Brookings Institution* (July 2015), 6, accessed March 18, 2016, http://www.brookings.edu/~/media/research/files/papers/2015/07/20-multistakeholder-internet-governance-brotman/multistakeholder.pdf.

[11] Evan Osnos, A*ge of Ambition: Chasing Fortune, Truth, and Faith in the New China,* Farrar, Straus and Giroux. Kindle Edition, 95.

[12] Li Xiguang and Wang Jing, “The Role of E-diplomacy in Iranian and Xinjiang Riots,” in *Media, Powerm and Politics in the Digital Age* edited by Yahya R. Kamalipour (Lanham, MD: Rowman and Littlefield Publishers, 2010), 148.

[13] Jing Li, “China blocks VPN services that let users get round its ‘Great Firewall’ during big political gatherings in Beijing,” *South China Morning Post,* March 9, 2016, accessed March 21, 2016, http://www.scmp.com/news/china/policies-politics/article/1922677/china-blocks-vpn-services-let-users-get-round-its-great.

[14] Ibid.

[15] Elsa Kania, “China's Military Strategy: A Cyber Perspective,” *Real Clear Defense,* June 3, 2015, accessed January 5, 2015, http://www.realcleardefense.com/articles/2015/06/03/chinas_military_strategy_a_cyber_perspective_108008.html.

[16] Lu Wei (鲁炜), “Jianchi zunzhong wangluo zhuquan yuance tuidong goujian wangluo kongjian mingyun gongtongti” [坚持尊重网络主权原则 推动构建网络空间命运共同体] (Adhere on respect for the principle of cyber sovereignty to promote and build cyberspace community of destiny), *Quishi,* February 29, 2016, accessed March 18, 2016, http://www.qstheory.cn/dukan/qs/2016-02/29/c_1118164592.htm.

[17] Li Minghai [李明海], “Dazao quanxin de wangluo ‘zuozhan liliang’,” [李明海：打造全新的网络“作战力量”] (Li Minghai: Forging a new network of ‘Combat Power’), *Morning Post,* accessed March 18, 2016, http://www.morningpost.com.cn/2016/0121/1246606.shtml.

[18] John Palfrey, “The end of the experiment: How ICANN's foray into global internet democracy failed,” *Harvard Journal of Law & Technology* 17, No. 2 (2004), 412.

[19] “Five Key Takeaways from ICANN 55,” *Mayer Brown Legal Update* (April 25, 2016), 1.

[20] Palfrey, “The end of the experiment: How ICANN's foray into global internet democracy failed,” 420.

[21] Amar Toor, “Will the global NSA backlash break the internet?” November 8, 2013, accessed May 14, 2016, http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization.

[22] Gui Tao, “China Voice: Time to reconsider Internet freedom touted by U.S.,” *Xinhua,* December 15, 2015, accessed March 21, 2016, http://news.xinhuanet.com/english/2015-12/15/c_134918998.htm.

NOTES

23. Zachary Keck, "Has Snowden Killed Internet Freedom?" *The Diplomat,* July 13, 2013, accessed May 13, 2016, http://thediplomat.com/2013/07/has-snowden-killed-internet-freedom/.

24. Hogan Lovells, "ICANN sets course for change of Internet stewardship," *LimeGreen IP* (April 7, 2016), accessed May 12, 2016, http://www.lexology.com/library/detail.aspx?g=b8f5da45-7169-4e39-9834-f84b9f318518.

25. Ibid., 3.

26. Stephen Karmazyn, "Deadline looms for U.S. to cede control over Internet naming conventions," *Globe and Mail,* May 8, 2016, accessed May 12, 2016, http://www.theglobeandmail.com/technology/deadline-looms-for-us-to-cede-control-over-internet-naming-conventions/article29933641/.

27. *Wuzhen Report on World Internet Development 2016* (November 18, 2016), accessed December 20, 2016, http://www.wuzhenwic.org/2016-11/18/c_61834.htm.

28. "China Cyber: Stepping Into the Shoes of a 'Major Power'," *EastWest Institute* (December 5, 2016), accessed December 20, 2016, https://www.eastwest.ngo/idea/china-cyber-stepping-shoes-"major-power"

29. Li Minghai, "Forging a new network of 'Combat Power'."

30. Bill Gertz, "PLA on cyberwarfare buildup," *Washington Times,* February 17, 2016, accessed March 20, 2016, http://www.washingtontimes.com/news/2016/feb/17/inside-the-ring-china-plans-cyberwarfare-force-to-/?page=all.

31. "Lun xinshiji xinjieduan wo jun de lishi shiming," [论新世纪新阶段我军的历史使命], *PLA Daily,* June 19, 2007, accessed March 9, 2016, http://news.xinhuanet.com/zgjx/2007-06/19/content_6262236.htm.

32. "Possible Push to Elevate US Cyber Command in Fight vs IS," *Voice of America,* April 5, 2016, accessed April 6, 2016, http://www.voanews.com/content/possible-push-elevate-us-cyber-command-fight-islamic-state/3270815.html.

33. Greg Masters, "Senate sends bill to Obama to elevate Cyber Command," *SC Media* (December 12, 2016), accessed December 19, 2016, https://www.scmagazine.com/senate-sends-bill-to-obama-to-elevate-cyber-command/article/578482/.

34. Laura Galante, "What To Watch: U.S.-China Cyber Talks Commence" *FireEye Blog* (December 11, 2015), accessed February 4, 2015, https://www.fireeye.com/blog/executive-perspective/2015/12/what_to_watch_u_s-.html.

35. Everett Rosenfeld, "US-China agree to not conduct cybertheft of intellectual property," *Reuters,* September 25, 2015.

36. Corey Bennett, "Obama talks cyber with Chinese President Xi Jinping," *The Hill,* March 31, 2016, accessed April 9, 2016, http://thehill.com/policy/cybersecurity/274845-obama-talks-cyber-with-chinese-president-xi-jinping.

37. "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," *Department Homeland Security* (December 7, 2016), accessed December 20, 2016, https://www.dhs.gov/news/2016/12/08/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

38. 2006 *Quadrennial Defense Review* (Washington, DC: US Department of Defense, February 6, 2006), 29.

39. 2014 *Quadrennial Defense Review* (Washington, DC: US Department of Defense, March 4, 2014), 7.

40. Franklin D. Kramer, Stuart H. Starr, Larry Wentz, *Cyberpower and National Security* (Kindle Edition: Potomac Books, 2009), 47.

41. Joint Publication (JP) 3-12(R) *Cyberspace Operations* (Washington, DC: Joint Staff, February 5, 2013), I-2.

42. David Raymond, Tom Cross, Gregory Conti and Michael Nowatkowski, "Key Terrain in Cyberspace: Seeking the High Ground," in *6th International Conference on Cyber Conflict* edited by P.Brangetto, M. Maybaum and J. Stinissen (Tallinn, Estonia: NATO CCD COE Publications, 2014): 298; Bryan Krekel, Patton Adams and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Report prepared for US-China Economic and Security Review Commission by Northrop Grumman Corp, Washington DC, March 7, 2012), 299.

43. David K. Edmonds, "In Search of High Ground: The Airpower Trinity and the Decisive Potential of Airpower," *Airpower Journal* (Spring 1998), accessed April 6, 2016, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj98/spr98/edmonds.html.

44. Ye Zheng, "Dui wangluo zhuquan de sikao," *Renmin Wanglilun* pindao, July 20, 2015, accessed January 9, 2016, http://theory.people.com.cn/n/2015/0720/c386965-27332547.html.

NOTES

45. An Weiping, "Deputy army commander: China should develop trump card forces," *China Military Online,* January 15, 2016, accessed March 22, 2016, http://english.chinamil.com.cn/news-channels/pla-daily-commentary/2016-01/15/content_6858982.htm.

46. Ibid.

47. Zhu Ningning, "Jiefangjun fujunzhang: jundui ying youxiao wangluo fankong renwu," [解放军副军长：军队应有效履行网络反恐任务] (Deputy Commander of the PLA: The PLA should carry out effective counterterrorism mission in cyberspace) *PLA Daily,* January 7, 2016, accessed March 22, 2016, http://www.chinanews.com/m/mil/2016/01-07/7705750.shtml.

48. An Weiping, "Deputy army commander: China should develop trump card forces".

49. Graham T. Allison and Morton H. Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics* 24, Supplement: Theory and Policy in International Relations (Spring 1972), 53.

50. Jerel A. Rosati, "Developing a Systematic Decision-Making Framework: Bureaucratic Politics in Perspective," *World Politics* 33, No. 2 (January 1981), 236.

51. Jason Healey, "Comparing Norms for National Conduct in Cyberspace," *New Atlanticist,* June 20, 2011, accessed January 9, 2016, http://www.atlanticcouncil.org/about/experts/list/jason-healey.

52. Internet Governance Progress After ICANN 53: Hearing Before Subcommittee on Communications and Technology Committee on Energy and Commerce United States House of Representatives, 114th Cong. (July 8, 2015) (Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, US Department of Commerce, Washington DC).

53. Nicholas Dynon, "The Future of Cyber Conflict: Beijing Rewrites Internet Sovereignty Along Territorial Lines," *Jamestown Foundation China Brief* 15, No. 17 (September 4, 2015), accessed January 10, 2016, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44338&cHash=1622a6ba07e8dfa6844d135dfaf073ad#.VpUI0pMrJE4.

54. Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," *Council on Foreign Relations,* December 16, 2015, http://blogs.cfr.org/cyber/2015/12/16/chinas-internet-conference-xi-jinpings-message-to-washington/.

55. Stuart N. Brotman, "Multistakeholder Internet governance: A pathway completed, the road ahead," *Brookings Institution* (July 2015), 6, accessed March 18, 2016, http://www.brookings.edu/~/media/research/files/papers/2015/07/20-multistakeholder-internet-governance-brotman/multistakeholder.pdf.

56. Huaxia, ed., "Highlights of Xi's Internet speech," *Xinhua,* December 16, 2015, accessed January 11, 2016, http://news.xinhuanet.com/english/2015-12/16/c_134923855.htm.

57. Ibid.

58. Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," translated by Yang Fan in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (London: Oxford Scholarship Online, April 2015), 132, doi:10.1093/acprof:oso/9780190201265.001.0001.

59. Ye Zheng, "Dui wangluo zhuquan de sikao," *Renmin Wanglilun pindao,* July 20, 2015, accessed January 9, 2016, http://theory.people.com.cn/n/2015/0720/c386965-27332547.html.

60. Scott D. Livingston, "Beijing Touts 'Cyber-Sovereignty' In Internet Governance: Global Technology Firms Could Mine Silver Lining," *ChinaFile* (February 19, 2015), accessed January 10, 2016, https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance.

61. *DoD Cyber Strategy* (Washington DC: Office of the Secretary of Defense, April 2015), 1.

62. *People's Republic of China Cybersecurity Law* (Draft), National People's Congress, accessed March 23, 2016, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

63. *Zhongguo de junshi zhanlüe* (Beijing: State Council Information Office of the People's Republic of China, May 2015), accessed January 8, 2016, http://www.scio.gov.cn/zfbps/gfbps/Document/1435341/1435341.htm.

64. "Xi pledges 'great renewal of Chinese nation'" *Xinhua,* November 29, 2012, accessed January 10, 2016, http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.

65. "Full Transcript: Interview With Chinese President Xi Jinping," *Wall Street Journal,* September 22, 2015, accessed January 10, 2016, http://www.wsj.com/articles/full-transcript-interview-with-chinese-president-xi-jinping-1442894700.

NOTES

66. "Chapter IV: Building and Development of China's Armed Forces," *China's Military Strategy* (May 26, 2015), accessed March 22, 2016, http://news.xinhuanet.com/english/china/2015-05/26/c_134271001_4.htm.

67. Luo Zheng [罗铮] "Junshi zhuanjia jiedu xinban guofang baipishu," [军事专家解读新版国防白皮书] (Military expert interpret the new defense white paper), *PLA Daily,* May 26, 2015, accessed March 22, 2016, http://jz.chinamil.com.cn/gd/2015-05/26/content_6507585.htm.

68. Song Xiaojun, "Zhongguo Xinban guofan baipishu 30 nianlai zui xiangxi," *Fenghuang xin meiti* (May 26, 2015), accessed January 14, 2016, http://v.ifeng.com/mil/mainland/201505/012b32da-beb1-4a9b-9d30-38d87c592420.shtml.

69. Yang Yucai, "White paper states China's peaceful intention," *Global Times,* May 5, 2015, accessed January 10, 2016, http://www.globaltimes.cn/content/924594.shtml.

70. Anthony H. Cordesman and Steven Colley, "Chinese Strategy and Military Modernization in 2015: A Comparative Analysis," *Center for Strategic and International Studies* (October 10, 2015), 121.

71. Toshi Yoshihara and James Holmes, Red Star over the Pacific: *China's rise and the challenge to US maritime strategy* (Annapolis, MD: Naval Institute Press, 2011), x.

72. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," CNA (February 2016), 5.

73. Luo Zheng, "Military expert interpret the new defense white paper."

74. Song Puxuan [宋普选], "Beibu zhanqu siling yuan: Jiajin qianghua suishi dahang huangtai" [北部战区司令员：加紧强化随时打仗状态] (Northern Military Region Commander: Intensifying and strengthening responsiveness for contingencies), *PLA Online,* March 15, 2016, accessed March 22, 2016, http://www.chinanews.com/mil/2016/03-15/7797840.shtml.

75. Huang Xiang [黄集骧], deputy director of political work for the Western Region, "Jujiao "zhuzhan" tuidong zhengzhi jiguan zhuanxing" [聚焦"主战"推动政治机关转型] (Focus on the "battle" to promote political reorganization), *PLA Online,* March 16, 2016, accessed March 22, 2016, http://www.81.cn/jfjbmap/content/2016-03/16/content_137936.htm.

76. Ben Lowsen, "How China Fights: The PLA's Strategic Doctrine," *The Diplomat,* April 6, 2016, accessed April 7, 2016, http://thediplomat.com/2016/04/how-china-fights-the-plas-strategic-doctrine/.

77. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," 1.

78. M. Taylor Fravel, "The evolution of china's military strategy: comparing the 1987 and 1999 editions of zhanlüexue," in *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army,* edited by James Mulvenon and David M. Finkelstein (Alexandria, Virginia: CNA, December 2005), 85.

79. Luo Zheng, "Military expert interpret the new defense white paper."

80. *China's Military Strategy* (US Naval Institute, May 26, 2015), accessed January 9, 2016, http://news.usni.org/2015/05/26/document-chinas-military-strategy.

81. David M. Finkelstein, "China's National Military Strategy," in *The People's Liberation Army in the Information Age* by James C. Mulvenon and Richard H. Yang, eds., (Santa Monica, CA: RAND Corporation, 1999), 103.

82. Ibid.

83. Derek S. Reveron and James L. Cook, "Developing strategists: Translating National Strategy into Theater Strategy," *Joint Forces Quarterly* 55 (4th Quarter 2009): 24.

84. Derek S. Reveron and James L. Cook, "Developing strategists: Translating National Strategy into Theater Strategy," 23.

85. Lin Dong [林东], "Guanyu zhanlüe xue chuangxin fazhan de sikao" [关于战略学创新发展的思考] (On the Innovative Development of the Science of Strategy), *Junshi Kexue* (April 1, 2014): 79.

86. Song Puxuan, "Northern Military Region Commander: Intensifying and strengthening responsiveness for contingencies".

87. Michael D. Swaine, "Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics," *China Leadership Monitor* 46 (March 19, 2015), 11, accessed January 10, 2016, http://www.hoover.org/research/xi-jinpings-address-central-conference-work-relating-foreign-affairs-assessing-and.

NOTES

88. Robert Lawrence Kuhn, “Xi Jinping’s Chinese Dream,” *New York Times,* June 4, 2013.

89. An, “Growing China to contribute more to Asia development: Xi,” *Xinhua,* October 29, 2014, http://news.xinhuanet.com/english/china/2014-10/29/c_133752083.htm.

90. Yin Pumin, “Mapping Out Success: New five-year blueprint lays down specific objectives for a prosperous China,” *Beijing Review* 45 (November 5, 2015), accessed January 10, 2016, http://www.bjreview.com.cn/Current_Issue/Editor_Choice/201511/t20151102_800041696.html.

91. Xi Jinping, “Working Together to Forge a New Partnership of Win-win Cooperation and Create a Community of Shared Future for Mankind,” Speech, United Nations, New York, NY, September 22, 2015, accessed January 10, 2016, http://qz.com/512886/read-the-full-text-of-xi-jinpings-first-un-address/.

92. Michael D. Swaine, “Xi Jinping’s Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics.”; Xi Jinping, “Chinese President Xi Jinping Addresses the American Public,” Speech, National Committee on U.S.-China Relations, Seattle, WA, September 22, 2015, accessed January 10, 2016, https://www.ncuscr.org/content/full-text-president-xi-jinpings-speech.

93. Wang Hongguang [王洪光], “Wang Hongguang tan lianghui: Bushi dongbeiya shengwen wei zhuyao zhanlüe fangxiang” [王洪光谈两会：不使东北亚升温为主要战略方向] (Northeast Asia is not the strategic direction that is heating up), *Sohu,* March 2, 2016, accessed March 19, 2016, http://mil.sohu.com/20160302/n439166845.shtml.

94. Ibid.

95. Wang Hongguang, “Lt. Gen. Wang Hongguang: no such thing as "giving up DPRK" for China,” *China Military Online,* December 2, 2014, accessed March 18, 2016, http://english.chinamil.com.cn/news-channels/china-military-news/2014-12/02/content_6251361.htm.

96. Yao Runping, ed., “President Hu Jintao asks officials to better cope with Internet,” *Xinhua,* January 24, 2007, accessed January 10, 2016, http://news.xinhuanet.com/english/2007-01/24/content_5648674.htm.

97. Wang Xixin [王西欣], “Zai lun kongzhizhan,” [再论控制战] (Further discussion on war of control), *Junshi Kexue* (April 15, 2014), 66.

98. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington DC: The Office of the President, May 2011), 5.

99. Adam Segal, “Chinese responses to the International Strategy for Cyberspace,” *Council for Foreign Relations* (May 23, 2011), accessed January 9, 2016, http://blogs.cfr.org/asia/2011/05/23/chinese-responses-to-the-international-strategy-for-cyberspace/.

100. Ye Zheng and Zhao Baoxian, “Wangluo zhan, zenme zhan?” *Zhongguo Qingnian bao,* June 3, 2011, accessed January 9, 2016, http://zqb.cyol.com/html/2011-06/03/nw.D110000zgqnb_20110603_1-09.htm.

101. *China’s Military Strategy* (US Naval Institute, May 26, 2015), accessed January 9, 2016, http://news.usni.org/2015/05/26/document-chinas-military-strategy.

102. Ibid.

103. *Zhongguo de junshi zhanlüe* (Beijing: State Council Information Office of the People's Republic of China, May 2015), accessed January 8, 2016, http://www.scio.gov.cn/zfbps/gfbps/Document/1435341/1435341.htm.

104. Luo Zheng, “Military expert interpret the new defense white paper”.

105. Franklin D. Kramer, Stuart H. Starr, Larry Wentz, *Cyberpower and National Security* (Kindle Edition: Potomac Books, 2009), 37.

106. Ibid.

107. 2006 *Quadrennial Defense Review,* 32.

108. US Cyber Deterrence Strategy (Washington DC: the White House, December 18, 2015), 3, accessed March 22, 2016, http://fedscoop.com/obama-cybersecurity-deterrence-strategy.

109. Michael Johnson and Terrence K. Kelly, “Tailored Deterrence: Strategic Context to Guide Joint Force 2020,” *Joint Forces Quarterly* 74 (3rd Quarter 2014): 26.

110. Rhea Siers, “The Myth of Cyber Deterrence,” *The Cipher Brief* (March 3, 2016), accessed March 22, 2016, https://www.thecipherbrief.com/article/techcyber/myth-cyber-deterrence.

NOTES

111. Peter Singer, "How the United States Can Win the Cyberwar of the Future: Cold War-era deterrence theory won't cut it anymore," *Foreign Policy,* December 18, 2015, accessed March 22, 2016, http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

112. Ibid.

113. Graham Webster, "America Can't Deter What It Can't Define in Cyberspace," *The Diplomat,* August 13, 2015, accessed March 22, 2016, http://thediplomat.com/2015/08/america-cant-deter-what-it-cant-define-in-cyberspace/.

114. Sarah Weiner, "Searching for Cyber-Deterrence," *Center for Strategic and International Studies* (November 26, 2012), accessed March 22, 2016, http://csis.org/blog/searching-cyber-deterrence/.

115. US *Cyber Deterrence Strategy*.

116. Lisa O. Monaco, "Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016," *White House* (February 2, 2016), accessed March 22, 2016, https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

117. Ibid.

118. Andrew Blake, "John McCain says White House's cyber deterrence policy comes up short," *Washington Times,* January 15, 2016, accessed March 22, 2016, http://www.washingtontimes.com/news/2016/jan/15/john-mccain-says-white-houses-cyber-deterrence-pol/.

119. Katie Bo Williams, "McCain blasts White House cyber policy," *The Hill,* January 15, 2016, accessed March 18, 2016, http://thehill.com/policy/cybersecurity/266104-mccain-blasts-white-house-cyber-policy.

120. Joint Publication (JP) 1-02 *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Joint Staff, February 15, 2016), 67.

121. Kevin Pollpeter, "Chinese Writings on Cyber Warfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (London: Oxford University Press, March 6, 2015), 147.

122. Rob de Wijk, *The Art of Military Coercion* (Amsterdam, NL: Amsterdam University Press, 2015), 17.

123. Thomas C. Schelling, Arms and Influence (Hartford, CT, USA: Yale University Press, 2008), 71-72.

124. Mingda Qiu, "China's Science of Military Strategy: *Cross-Domain Concepts in the 2013 Edition," Cross-Domain Deterrence (CCD) Working Paper UC San Diego* (September 2015): 10.

125. Dennis J. Blasko, *The Chinese Army Today: Tradition and Transformation for the 21st Century* (New York, NY: Routledge, 2012), 231.

126. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," 53.

127. Larry M. Wortzel, *The Dragon Extends its Reach* (Kindle Edition: Potomac Books, 2013), Kindle Locations 1550-1551.

128. Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC" (Lecture delivered at the Heritage Foundation, Washington DC, January 21, 2016), 2.

129. Kevin Pollpeter, "Chinese Writings on Cyber Warfare and Coercion."

130. Yuan Yi [袁艺], "Qian xi wangluo kongjian weishe de teheng, leixing he yunyong yaodian," [浅析网络空间威慑的特征、类型和运用要点] (The characteristics, types, and applications of cyberspace deterrence), *People's Daily,* January 4, 2016, accessed March 19, 2016, http://theory.people.com.cn/n1/2016/0104/c386965-28010082.html.

131. Ibid.

132. Yuan Yi, "The characteristics, types, and applications of cyberspace deterrence."

133. Bill Gertz, "Cyber 'People's War' On U.S.," *Washington Times,* June 4, 2014, accessed May 12, 2016, http://m.washingtontimes.com/news/2014/jun/4/inside-the-ring-hagel-to-testify-before-house-pane/.

134. Adam Segal, "From China, an Expansive and Dangerous View of Cyber Deterrence," *Defense One* (January 26, 2016), accessed March 22, 2016, http://www.defenseone.com/threats/2016/01/china-expansive-and-dangerous-view-cyber-deterrence/125418/.

135. Ibid.

NOTES

136. Joseph Marks, "U.S. may punish Chinese hacking before Xi's visit," September 4, 2015, *Politico,* accessed March 23, 2016, http://www.politico.com/story/2015/09/white-house-chinese-cyber-sanctions-xi-jinping-visit-213360.

137. Erin Kelly, "OPM's cybersecurity chief resigns in wake of massive data breach," USA *Today,* February 22, 2016, accessed March 23, 2016, http://www.usatoday.com/story/news/2016/02/22/opms-cybersecurity-chief-resigns-amid-continuing-pressure-congress/80766320/.

138. Evan Perez, "U.S. pulls spies from China after hack," *CNN,* September 3, 2015, accessed March 23, 2016, http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/.

139. Jonathan Chew, "China Says It Wasn't Behind the Massive U.S. Government Hack," *Fortune,* December 2, 2015, accessed March 23, 2016, http://fortune.com/2015/12/02/china-opm-hack/.

140. Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," *Washington Post,* December 2, 2015, accessed March 23, 2016, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

141. Aliya Sternstein, "NSA director: expect more hacks as big as the OPM heist," *Nextgov,* January 22, 2016, accessed March 23, 2016, http://www.nextgov.com/cybersecurity/2016/01/nsa-director-expect-more-hacks-big-opm-heist/125320/.

142. Colin Clark, "DNI Clapper IDs China As 'The Leading Suspect' In OPM Hacks; Russia 'More Subtle'," *Breaking Defense,* June 25, 2015, accessed March 23, 2016, http://breakingdefense.com/2015/06/clapper-ids-china-as-the-leading-suspect-in-opm-hacks-russia-more-subtle/.

143. Damian Paletta, "Former CIA Chief Says Government Data Breach Could Help China Recruit Spies," *Wall Street Journal,* June 15, 2015, accessed March 23, 2016, http://www.wsj.com/articles/former-cia-chief-says-government-data-breach-could-help-china-recruit-spies-1434416996.

144. Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *New York Times,* September 25, 2015, accessed March 23, 2016, http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

145. Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement," *Council for Foreign Relations,* January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

146. Kris Klein, "Cyber Sovereignty: The economic imperatives of a secure cyberspace," *Prospect: Journal of International Affairs at UCSD* (November 17, 2015), accessed March 23, 2016, http://prospectjournal.org/2015/11/17/cyber-sovereignty-the-economic-imperatives-of-a-secure-cyberspace/.

147. "Chinese President underscores cyber sovereignty, rejects Internet hegemony," *Xinhua,* December 16, 2014, accessed March 23, 2016, http://news.xinhuanet.com/english/2015-12/16/c_134922689.htm.

148. Jack Goldsmith, "U.S. Attribution of China's Cyber-Theft Aids Xi's Centralization and Anti-Corruption Efforts," *Lawfare* (June 21, 2016), accessed August 15, 2016, https://www.lawfareblog.com/us-attribution-chinas-cyber-theft-aids-xis-centralization-and-anti-corruption-efforts.

149. Ibid.

150. Gregory Kulacki, "The Chinese Military Updates China's Nuclear Strategy," *Union of Concerned Scientists* (March 2015), 5, accessed March 18, 2016, http://www.ucsusa.org/sites/default/files/attach/2015/03/chinese-nuclear-strategy-full-report.pdf.

151. Peter Dutton, "Viribus Mari Victoria? Power and Law in the South China Sea" (Paper submitted for "Managing Tensions in the South China Sea" conference, Center for Strategic and International Studies, June 5-6, 2013), 6.

152. Ibid.

153. Ibid.

154. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security 39,* No. 3 (Winter 2014/15): 7-47, doi: 10.1162/ISEC_a_00189.

155. Jon R. Lindsay, "Exaggerating the Chinese Cyber threat," *Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School* (May 2015), accessed March 12, 2015, http://belfercenter.ksg.harvard.edu/files/linsday-china-cyber-pb-final.pdf.

NOTES

156. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction."

157. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 4.

158. Allen Suess Whiting, China crosses the Yalu: *The decision to enter the Korean War* (Stanford University Press, 1968), 156.

159. Richard W. Stewart, "The Chinese Intervention," in *The Korean War* (US Army Center of Military History, March 8, 2002), 33.

160. National Security Council Report, NSC 81/1, "United States Courses of Action with Respect to Korea," September 9, 1950, accessed March 12, 2016, http://digitalarchive.wilsoncenter.org/document/116194.

161. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 94.

162. Ibid, 106.

163. Ibid, 111.

164. Ibid, 121.

165. Ibid, 132.

166. Ibid.

167. Ibid.

168. "Korean War Fast Facts," CNN, July 3, 2015, accessed March 23, 2016, http://www.cnn.com/2013/06/28/world/asia/korean-war-fast-facts/.

169. David Shambaugh, "PLA Strategy & Doctrine: Recommendations for a Future Research Agenda" (Discussion paper prepared for "Chinese Military Studies: a Conference on the State of the Field" at the US National Defense University Institute for National Strategic Studies' Center for the Study of Chinese Military Affairs, Fort McNair, Virginia, October 26-27, 2000), accessed March 12, 2016, http://www.comw.org/cmp/fulltext/0010shambaugh.htm.

170. Cheng Jun (程军), "Huayang diechu de meijunjunshi lilun: Jiduo shi tansuo jiduo shi huyou" [Persistent patterns of US military doctrine: How much is exploration? How much is manipulation?] *PLA Daily,* October 14, 2010, accessed March 16, 2016, http://theory.people.com.cn/GB/12954938.html.

171. Joint Chiefs of Staff J7, "The Role of Multinational Joint Doctrine," *Joint Forces Quarterly,* no. 67 (4th Quarter, 2012), 111.

172. Alison A. Kaufman and Peter W. Mackenzie, "Field Guide: The Culture of the Chinese People's Liberation Army," 25.

173. Christopher P. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations* (Ithaca, NY: Cornell University Press, 2010), 243.

174. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 243.

175. Graham Webster, "America Can't Deter What It Can't Define in Cyberspace," *The Diplomat,* August 13, 2015, accessed March 22, 2016, http://thediplomat.com/2015/08/america-cant-deter-what-it-cant-define-in-cyberspace/.

176. 2015 *National Military Strategy* (Washington DC: Joint Staff, June 2015), 4.

177. Ibid.

178. Ibid.

179. TRADOC Pamphlet 525-3-1 *US Army Operating Concept: Winning in a Complex World 2020-2040* (Washington, DC: Army Staff, October 31, 2014), 7.

180. Ibid, 16.

181. Wang Xixin [王西欣], "Zai lun kongzhizhan," [再论控制战] (Further discussion on war of control), *Junshi Kexue* (April 15, 2014), 64.

182. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," *CNA* (February 2016), 1.

183. Lin Dong [林东], "Guanyu zhanlüe xue chuangxin fazhan de sikao" [关于战略学创新发展的思考] (On the Innovative Development of the Science of Strategy), *Junshi Kexue* (1 April 2014), 79.

184. Adam Segal, "Stabilizing Cybersecurity in the U.S.-China Relationship," *Council for Foreign Relations* (September 14, 2015), accessed March 12, 2016, http://nbr.org/research/activity.aspx?id=605.

185. Ibid.

NOTES

186. General Assembly resolution 64/211, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, A/RES/64/211/Add 3 (December 21, 2009).

187. Cheryl Pellerin, "U.S., China Must Work Together on Cyber, Panetta Says," *American Forces Press Service – DoD News,* May 7, 2012, accessed March 12, 2016, http://archive.defense.gov/news/newsarticle.aspx?id=116235.

188. Michele Markoff, "Developments of Cyberspace and Emerging Challenges" (Remarks for panel session at ARF Workshop on cyber capacity building, Beijing, China, July 28, 2015), accessed March 12, 2016, http://beijing.usembassy-china.org.cn/mobile/2015/arf-workshop-on-cyber-capacity-building.html.

189. "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track," *US Department of State* (July 14, 2014), accessed March 13, 2016, http://www.state.gov/r/pa/prs/ps/2014/07/229239.htm.

190. Xu Lin, "Zhongmei duihua you zhu zengxinshiyi," [US-China Dialogue will help enhance mutual trust] *PLA Daily,* July 10, 2014, accessed March 13, 2016, http://navy.81.cn/content/2014-07/10/content_6041990.htm.

191. Takeshi Yamawaki, "Interview/ Kurt Campbell: China should think carefully about provoking South China Sea tensions," *Ashi Shimbun,* June 20, 2015, accessed January 15, 2016, http://ajw.asahi.com/article/views/opinion/AJ201506200060.

192. Kimberly Field and Stephan Pikner, "The Role of U.S. Land Forces in the Asia-Pacific," *Joint Forces Quarterly* 74 (3rd Quarter 2014), 33.

193. Ibid.

194. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, Washington DC, September 25, 2015, accessed March 12, 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

195. "Xinjinping chuxi baigong huanying yishi aobama zhongwen shuo 'ni hao' zhiyi," [习近平出席白宫欢迎仪式 奥巴马中文说"你好"致意], *China National Radio,* September 26, 2015, accessed March 13, 2016, http://china.cnr.cn/yaowen/20150926/t20150926_519982837.shtml.

196. Graham Webster, "Has U.S. Cyber Pressure Worked on China? Read those leaks carefully," *The Diplomat,* December 10, 2015, accessed March 13, 2016, http://thediplomat.com/2015/12/has-u-s-cyber-pressure-worked-on-china/.

197. *US Cyber Deterrence Strategy,* 5.

The Challenge of Security – West Point's Defenses and Digital Age Implications, 1775-1777

Dr. Nicholas Michael Sambaluk

ABSTRACT

Although the cyber realm is a comparatively new environment, with professionals typically setting the origins in the mid-19th century with the communications network established in support of the Anglo-French-Piedmontese force in the Crimean War, many of the imperatives of security and defense in the physical realm offer significant continuity as well as areas for profitable comparison. The historical vantage point empowers, through the use of relevant analogy and studious research and analysis. A cyber-conscious study of the early progress toward fortification of the Hudson River during the American Revolutionary War illuminates themes about the primary security role played by defensive constructions: to guarantee time that permits an active and coherent response against an adversary. It also demonstrates the vital role played by leaders who recognize security challenges and the need for expertise that can translate policymakers' support and resources into an effective security system. This essay uses the period from 1775-1777 to highlight these issues, setting the stage for the development of expert-designed fortress construction beginning in the spring of 1778 (to be examined in the author's next contribution to the CDR).

INTRODUCTION

West Point's history as a layered defensive network and the security challenges its designers and personnel confronted offer useful areas for consideration when working to pursue cyber security. Interesting and significant parallels exist between the physical security challenges of the 18th century, and the attitudes and approaches to solving them on the one hand, and more modern problems and answers. Despite the differences in time and environment, multifaceted and relevant historical analogies and case studies contribute key tools in building a fuller and more meaningful understanding of new security environments.[1] The events surrounding the early period of Hudson

Dr. Nicholas Michael Sambaluk is an Assistant Professor of Comparative Military Studies at the Air Command and Staff College at Maxwell Air Force Base. He taught military history at Purdue University during the 2015-16 school year and served as a Liaison for Cyber Research for the Army Cyber Institute at West Point from 2014 to 2016. From January 2013 through May 2015, he served on the USMA history department faculty. His first book, *The Other Space Race: Eisenhower and the Quest for Aerospace Security* (Naval Institute, 2015), explored the pursuit of effective security policy, and his writing also appears as part of *Cyber Warfare: A Reference Handbook* (ABC-CLIO, 2015) and in the journal Cold War History.

River fort construction, from 1775 through 1777, suggest crucial points about key early actions and mindsets toward establishing security.

ORIENTATION TO WEST POINT

From the modern site of the Kosciuszko Monument, it is possible to get a clear sense of why West Point was once considered to be perhaps the most important single strategic point in the United States. Looking out to the river, we can see the Hudson River, a tidal waterway and one of the key transportation and communication avenues on the Atlantic seaboard. It leads, to the far right (south) to New York City, and the Hudson is essentially a straight north-south line the 44 miles to New York City.

Why does that matter? Because defending the river means slowing that enemy down long enough to shoot at it. In the days of wooden ships traveling by sail, the ship (simultaneously a weapons technology and a communication technology) is most vulnerable when attempting to turn or when adjusting to a turn in the wind. Since the local weather is practically beyond human manipulation, the best defensive geography is a place where the terrain itself forces the ship to slow down, deploy its sailors at the rigging (and therefore not at its cannon) to help the ship turn. Nodes and bottlenecks are just as significant in manufactured spaces as they are among natural terrain features.

The strength of this spot now becomes clearer. To the left, we see a projection of land, known as Constitution Island, which creates two bends in the river. A ship must make first one abrupt 90-degree turn to the left, and then another turn just as sharply to the right, within a few hundred meters.

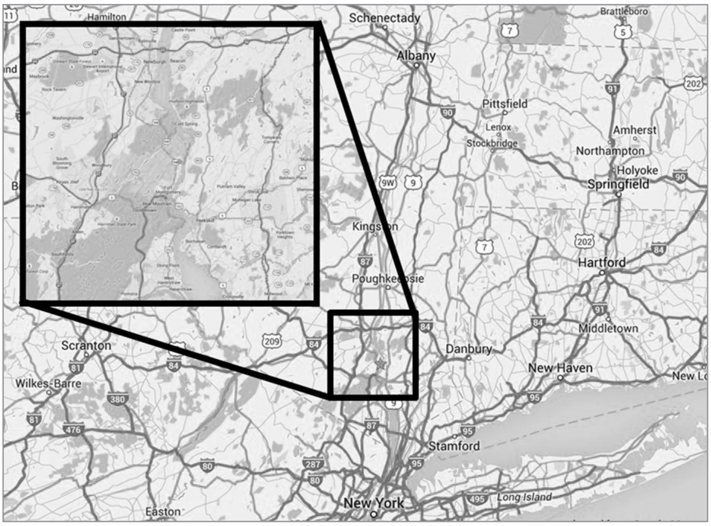
That is going to keep a ship and its crew busy. It makes for a slow-moving and vulnerable target. This is good news, and vital for anyone trying to defend upstate New York or inland New England from invasion.

Within six weeks of the shots at Lexington and Concord that marked the start of the American Revolutionary War, the Continental Congress realized the extreme importance of preventing the Hudson River from falling into British hands.[2] The matter was so serious that the Congress identified the need to defend the Hudson by May 1775—weeks before they had even embraced the idea that the American cause would need a formal army. They feared, and the British hoped, that capture of New York City and the Hudson River might slice away the northeastern Colonies that represented the heart of the rebellion. The Congress, therefore, dispatched two men, Christopher Tappan and James Clinton, to survey the Hudson River and search for the best candidate areas for establishing a fortress.

It is important for us to recognize that the first job of a fortress, whether here or anywhere else on the planet, is to establish a military presence and enable friendly forces to delay an enemy conquest. No fortress was ever built with an eye toward holding out forever, and there is no fortress ever built which could do so.[3] This applies to physical defenses just as much as in the world of cryptology or of cybersecurity: defenses buy time.

Time for what? Hopefully, time for friendly entities to be warned, informed, mobilized, and launch an action to reverse the effect of whatever inroads an intruder has made. The best defenses are those matching the needs and resources of the defender, and those needs are impacted by the enemies and technologies the defender expects to face. This also is true whether the defenses are physical, electronic, or intellectual.

Tappan and Clinton identified three candidate sites in this area. Two were a few miles to the south and were much less inviting for a defender: the river was wide, and its bend was subtle. In contrast, the area around the west point (a rock across the Hudson River from Constitution Island) appeared to have everything a defender might require.



The Hudson River's path ending New York City and beginning north of Albany. A tidal body for much of its length, the Hudson is deep enough to be navigable by many ocean-going vessels, and at few spots does the river bend appreciably enough to complicate transit. The only substantial challenges exist at the sites adopted for the West Point and Fort Montgomery defenses.

Almost everything.

The site where the Kosciuszko Monument stands is in itself a poor place for an 18th century fort to directly guard the Hudson River. Standing on a tall bluff, it gives an excellent view of the river, but that was part of the problem. Eighteeth century firearms had smooth bores and projectiles were driven by black powder. Black powder does not have a precisely consistent force, so two cannons firing a ball pushed by the same amount of powder may not land in the same spot. Furthermore, a smoothbore gun uses gravity to keep the projectile in the barrel. Firing a cannon from a height would mean either depressing a gun so much that the cannon ball would roll out before firing, or lobbing a cannon ball by a steep trajectory as if it were a mortar. Ten years later, the British defending Gibraltar would make some strides in successfully depressing smoothbore cannon, but this was not an option to American defenders in 1775. Firing a cannon like a mortar would accentuate all the problems of black powder's limitations. Therefore, a clear view of the river does not equal a clear choice of location for building a fortress.

EARLY WORK ON HUDSON RIVER DEFENSE

Tappan and Clinton opted instead for Constitution Island, on the east bank, where its low elevation would circumvent the thorny artillery challenges. But another inevitable problem arose. The United States (more accurately, the rebellious colonies, since the Declaration of Independence had not yet been written) did not have any indigenous military engineering experts. Tappan and Clinton found the next closest thing, which wasn't close. Bernard Romans was Dutch by birth, later a British subject, and an American sympathizer by 1775. Although scientific fields were not differentiated quite as they would become later, Romans was essentially a botanist, whose work had also involved civilian architecture and engineering.[4] By no stretch of the imagination did he have prior experience building fortresses, and fortress design and construction in Europe had been refined to a geometric and terrain-reading science since at least the time of Sebastien de Vauban, who in the late 17th century had girded France in belts of intricate and robust fortifications. Romans accepted Tappan and Clinton's recommendations to site the fort on the east back, and he set to work throughout 1776.

> From the modern site of the Kosciuszko Monument, it is possible to get a clear sense of why West Point was once considered to be perhaps the most important single strategic point in the United States.

New to an established and demanding field, Romans' efforts led him to sketch elaborate concepts. He did so, in part, because he encountered what trained military engineers had been taught: that any defensive position is completely compromised by a single significant weakness. Romans' solution led him to fortify (on paper) more and more, until his drawings called for a stone defensive position armed with more than 60 cannons. About two-thirds of these would be pointed at the river, and the rest would defend against landward attack. [5]

Romans' plan had several serious challenges. One obvious difficulty was that the Americans did not possess enough cannon to fill his proposed fort. The United States (which had declared its independence during the intervening months) did not have any cannon manufacturers and had only limited access to guns smuggled or imported from European states envious of Britain but by no means confident in the upstart country's chance of success. The fall of Fort Ticonderoga, orchestrated by an American officer Benedict Arnold and a Vermont leader Ethan Allen, had transformed the fort's armory into a modest source of cannon for all of the country's needs. Understandably, regarding limited equipment, weapons, and personnel, Washington's army in the field took precedence over a would be fortress location that was not yet imminently threatened. [6] By mid-1776, forty-one cannons were available, [7] but these were light field guns with calibers too small to offer any serious threat to a warship. The garrison, which doubled as the labor for improving the fort, comprised just 160 personnel who were "miserably armed," as at least a quarter of the firearms were rusted and "in very bad order." [8]

The best defenses match the needs and resources of the defender, and those needs impact the enemies and technologies the defender faces.

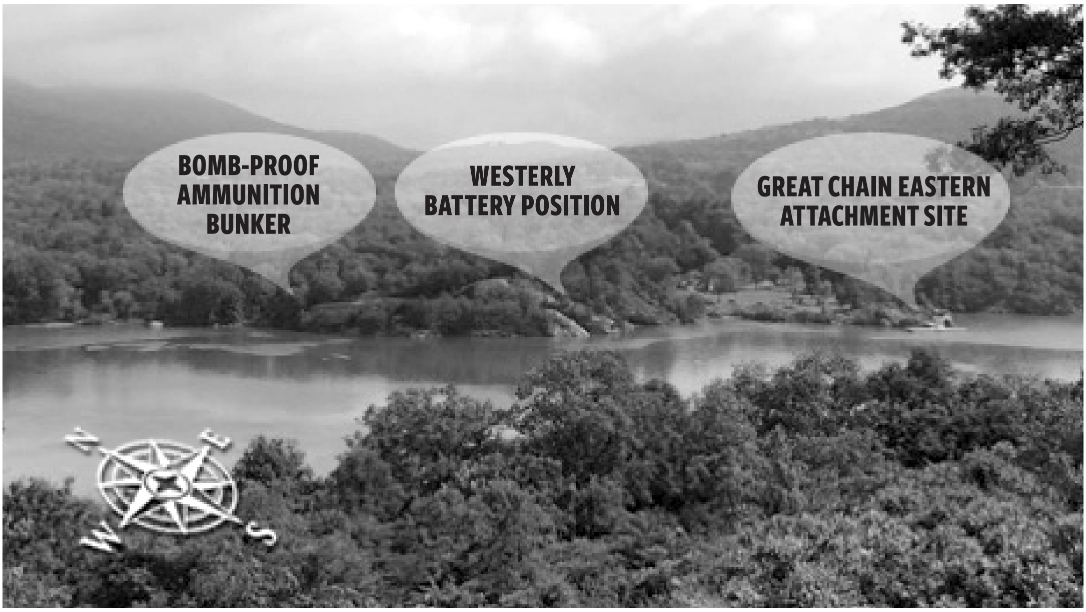
Other problems were more avoidable. Romans demanded an extensive masonry complex at a time and place that lacked craftsmen able to do the work. The Hudson Valley was still a fairly rural area, and although rock was available, stonemasons were not. More avoidable still was Romans' restive refusal to update the state's authorities (this was after all seen as New York's responsibility first and a national responsibility second) about his progress and budget. The budget was a serious problem. A year after starting the project, Romans had committed £5000, when his allotted budget had been just £1500. By the end of 1776, Romans had been fired. [9]

ANALYZING THE DEFENSES

Before Romans' removal, American General William Alexander, known as Lord Sterling, inspected the status and progress of the Hudson River fortifications. These consisted of Romans' efforts at Fort Constitution on the east bank of the Hudson across from West

Point, as well as a pair of stone works a few miles to the south. There, local militia constructed two stone works they called Fort Montgomery and Fort Clinton, which straddled a tributary on the west bank of the Hudson. The forts were essentially low stone enclosures, laid out with little trained forethought. Again, this was less the result of negligence insteadof the mercantile-colonial environment not facilitating the development of military engineering know-how in the colonies. Stirling identified the particularly in expert dispositions of Fort Montgomery and Fort Constitution, which in both cases, were surrounded by terrain features that would make the fort's further defense untenable if they were occupied by the enemy. Stirling's visit in May 1776 coincided with the first anniversary of American attention toward defending the Hudson River.

The Hudson River defenses in the vicinity of West Point consisted of four artillery battery positions. Of these, two covered the approach that northbound ships would take up the river, another assisted river defense to a lesser degree, and the fourth was positioned far enough to the west that it would have a clear line of fire only at ships which had already completed the first of the two ninety degree turns dictated by the river. As such, Stirling noted, the fourth battery could "only annoy a Ship going past," despite the considerable cost of construction. Romans' aptitude for civilian architecture was evident in his aptitude for military design, as Stirling's report to General George Washington noted a wooden tower with garret windows that "looks very picturesque, upon the whole Mr Romans has


BOMB-PROOF AMMUNITION BUNKER
WESTERLY BATTERY POSITION
GREAT CHAIN EASTERN ATTACHMENT SITE
N
E
W
S

A view eastward across the Hudson River, from the west point toward Constitution Island. As designed, Fort Constitution was too expensive to build, required too many artillery pieces, and would be positioned too awkwardly along the river's first curve to impose major challenges to an enemy warship. **Photo Credit: Dr. Nicholas M. Sambaluk** displayed his Genius at a very great Expence, [*sic*] & very little publick [*sic*] Advantage."[10] Given the scarcity of funds, materials, and craftsmen, this "great Expence" was an enormous problem.

Perhaps worst of all, Fort Constitution was dominated by nearby terrain. Stirling bluntly explained that "every work on the Island is Commanded by the Hill on the West point [*sic*] ... a Redoubt on this West point [*sic*] is absolutely necessary, not only for preservation of Fort Constitution but for it's [*sic*] own importance on many accounts." The general believed that "One good Engineer with Artificers from the Army" would do a great deal to improve "the whole Business."[11] The situation overall was one of flawed design, inadequate materials, and above all a lack of specialist know-how to direct and execute construction of a defensive system capable of meeting enemy efforts and delaying the enemy's passage and exploitation for long enough that the defenders could rally and respond. Lieutenant Colonel Henry Beekman Livingston agreed entirely with Stirling's estimate, explaining that "the work of most Consequence is Excluded, as it Commands at Point Blank All the fortifications Erected on this Island." As a stopgap before more permanent positions could be developed, Livingston urged the construction "immediately" of some hasty defensive position "on a Point Call'd West Point."[12]

One vital continuity is the purpose of defensive systems: a defense is built to buy time for the defender, and crucially to buy time for the defender to take positive action.

"Difficulties and Obstacles" had slowed construction of the vital forts and troubled Washington, but with the Revolutionary main army requiring his attention and command, he was compelled to cite his unfamiliarity with the minutiae of the Hudson Valley's geography when a secret committee of New York patriot officials requested his "advice on this important subject."[13] However, the situation throughout the rest of 1776 and 1777 remained one characterized by the deplorable lack of progress. In fact, the ongoing problem of material shortages even prompted moves to redirect building resources and ordnance from one fortress project to another.[14] Nonetheless, along the Hudson River, the forts' wishful builders had presumably expected that state militia would throng to defend the forts upon notice of a British move up the river.

THE CRISIS

Other problems beset the American cause, stemming from a shortage military intelligence, uneven generalship, and indiscipline with Washington confiding to his brother John in the hard autumn of 1776: "I am wearied almost to death with the retrog[r]ade

Motions of things,"[15] Inadequate military intelligence contributed to major problems the next summer, when General Washington assured American Major General Israel Putnam that British forces under Major General William Howe made it "beyond all matter of doubt, that he has dropped all thoughts of an expedition up the North [Hudson] River," just days before British redeployments forced Washington to reverse himself and conclude that "Hudsons [*sic*] River seems to be the Object of his attention."[16] A British contingent under Major General Henry Clinton (not to be confused with the James Clinton who surveyed the Hudson or the governor George DeWitt Clinton who commanded state militia and was the namesake of one of the river's forts). The militia who rallied to the forts found that their numbers were too few to adequately defend both Fort Clinton and Fort Montgomery, and realized that both works were also too insubstantial to be defended for long. Nonetheless, the American force attempted to hold both sites on the west bank. When Henry Clinton sent a group of Tory militia overland to assault the forts from the landward sides and had warships approach on the river, the American defenses promptly collapsed, and the garrisons were killed or captured. A small contingent of 120 militia at Constitution Island unleashed a volley on a small party of British personnel later in the day and fled at nightfall.[17]

A view from Fort Constitution's artillery battery site, looking across the Hudson River to the far shore—a position that gave West Point its name. **Photo Credit: Dr. Nicholas M. Sambaluk**

If not for the nearly simultaneous reduction of John Burgoyne's army near Saratoga, the British would have effectively captured the Hudson River in October 1777. The American defenses along the river were utterly destroyed by Henry Clinton's modest force. The absence of instant communication spared the Americans the consequences of the British success on the Hudson River, as Clinton's British force was unaware of the dire predicaments facing Burgoyne's larger invading army barely 100 miles away.

At the climax of the crisis, Washington ordered a French officer dispatched to assist the American cause, Lieutenant Colonel Lewis de la Radiere, “to Fort Montgomery” to “take upon you the direction of such Works as shall be deemed necessary by the commanding Officer in that department.” [18] When issuing the order, Washington did not yet know that Fort Montgomery had just fallen to the British contingent under Henry Clinton. [19] The British presence ended when they returned to New York City in late October to establish winter quarters. Given the frequent confusion of the various Hudson River forts, it is likely that Washington had in mind that Radiere would as a trained military engineer oversee construction in the entire area, including Fort Constitution and the as-yet unimproved area on the west bank.

American militia returned to the site of Constitution Island, now abandoned by the British. On January 27, 1778, American personnel crossed to the western bank of the river. Then, as now, the Hudson Valley is inhospitable terrain at the height of its winter, and after a few hours’ presence, they returned to their camp on the east bank. Their return, three days later, marked the beginning of the US Army’s permanent presence at its oldest continuously operated post. [20]

News of the American victory at Saratoga had an important impact on the defense of the Hudson. Certainly, the northern invasion threat disappeared and helped convince France’s Louis XVI to enter a war that would (unbeknownst to him) further ensure revolution in his own a decade later. The formal French alliance made possible the delivery of French guns, ultimately of French sailors and soldiers, and also of French engineering experts. Covert French aid had already included a small cadre of desperately needed foreign officers with training and experience in military engineering. Lieutenant Colonel la Radiere, twice promoted in exchange for acceding to travel to America, was among this group. The American victory at Saratoga simultaneously opened the potential of releasing military units involved in Burgoyne’s defeat that fall. The dearth of trained military engineers at West Point was coming to an end. An inverse problem arose, as the Hudson Valley would soon find that it had too many cooks in the kitchen.

> No fortified construct, whether physical or digital can be relied upon to hold off an attacker indefinitely.

CONCLUSION

What cyber lessons, parallels, and contrasts, can be identified in this exploration of the early fortification of the Hudson River? One vital continuity is the purpose of defensive systems: a defense is built to buy time for the defender, and crucially to buy time for the defender to take positive action. No fortified construct, whether physical or in a digital environment, can be relied upon to hold off an attacker indefinitely. This point will be explored further in the second part of this project. A significant distinction between cyber and physical environments is that the terrain in a cyber environment is “built, not born.” [21] This is undeniably true, although it is useful to remember that the construction of defenses (both cyber and physical) is a deliberate activity.

That deliberate action presupposes coordinated action. This initial action frequently has to occur before it is yet clear how best a challenge can be overcome—the identification itself is a necessary early step across different environments. The Continental Congress identified the need for Hudson River defenses even before it could agree to establish a United States Army. NATO members’ identification of cybersecurity dangers is a precondition of effectively meeting those requirements. [22]

Translating these vital elements into an effective and coherent system is a complex challenge. Examining the organized planning, tangible development, and functioning maintenance of secure systems from 1778 through 1781 provides a lens through which to engage with these issues.

NOTES

[1] Ty Seidule, "Conclusion," *Stand Up and Fight! The Creation of US Security Organizations,* 1942-2005, ed. Ty Seidule and Jacqueline E. Whitt (Strategic Studies Institute, 2015), 257-8.

[2] Charles E. Miller, Donald V. Lockey, and Joseph Visconti, *Highland Fortress: The Fortification of West Point During the American Revolution, 1775-1783* (United States Military Academy, 1979), 15.

[3] For a sample of the discursive study about the role and purpose of fortresses, and the terms in which these issues are currently presented to USMA cadets in their study of military history, see John Lynn's "Chapter 5: The French Army and the Wars of Louis XIV, 1661-1688" in *The West Point History of Warfare,* ed. Clifford Rogers and J.T. Seidule (Rowan Technologies, 2014), 25-29.

[4] David Richard Palmer, *The River and the Rock: The History of Fortress West Point, 1775-1783* (Greenwood, 1969), 32.

[5] Miller, et al, *Highland Fortress,* 18-21.

[6] George Pappas, *To The Point: The United States Military Academy,* 1802-1902 (Praeger, 1993), 6.

[7] Footnote 9, *The Papers of George Washington: Revolutionary War Series 4, April-June 1776,* ed. Philander D Chase (University Press of Virginia, 1991), 423.

[8] From Lord Stirling [to George Washington], 1st June 1776, *The Papers of George Washington: Revolutionary War Series 4,* 420-1.

[9] Miller, et al, *Highland Fortress,* 46.

[10] From Lord Stirling [to George Washington], 1st June 1776, *The Papers of George Washington: Revolutionary War Series 4,* 418-20.

[11] From Lord Stirling [to George Washington], 1st June 1776, *The Papers of George Washington: Revolutionary War Series 4,* 420-23.

[12] From Lieutenant Colonel Henry Beekman Livingston [to George Washington], June 11th-14th, 1776, T*he Papers of George Washington: Revolutionary War Series 4,* 502.

[13] From a Secret Committee of the New York Convention [to George Washington], 17th July 1776, The Papers of *George Washington: Revolutionary War Series 5,* June-August 1776, ed. Philander D Chase (University Press of Virginia, 1993), 361; To a Secret Committee of the New York Convention [from George Washington], July 19, 1776, *The Papers of George Washington: Revolutionary War Series 5,* 391-2.

[14] Thomas Machin to General Putnam, 25th July 1777, *Public Papers of George Clinton, First Governor of New York, 1777-1795 – 1801-1804, Volume II* (New York: Wynkoop Hallenbeck Crawford, 1900), 133. From Lieutenant Colonel Henry Beekman Livingston [to George Washington], June 11th-14th, 1776, *The Papers of George Washington: Revolutionary War Series 4,* 501.

[15] To John Augustine Washington [from George Washington], Nov 6-9, 1776, *The Papers of George Washington, Revolutionary War Series 7, October 1776-January 1777,* ed. Philander D. Chase (University Press of Virginia, 1997), 105.

[16] To Major General Israel Putnam [from George Washington], 12th June 1777, *The Papers of George Washington, Revolutionary War Series 10, June-August 1777,* ed. Philander D. Chase (University Press of Virginia, 17; To Major General William Heath [from George Washington] July 4th, 1777, *The Papers of George Washington, Revolutionary War Series 10,* 189.

[17] Theodore J. Crackell, *West Point: A Bicentennial History* (University of Kansas, 2002), 11-12.

[18] To Lieutenant Colonel La Radiere [from George Washington] 8th October 1777, *The Papers of George Washington, Revolutionary War Series 10,* 440.

[19] George Clinton to George Washington, 9 October 1777, *Public Papers of George Clinton, Volume II,* 380.

[20] Crackell, 12.

[21] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, 2007), 5.

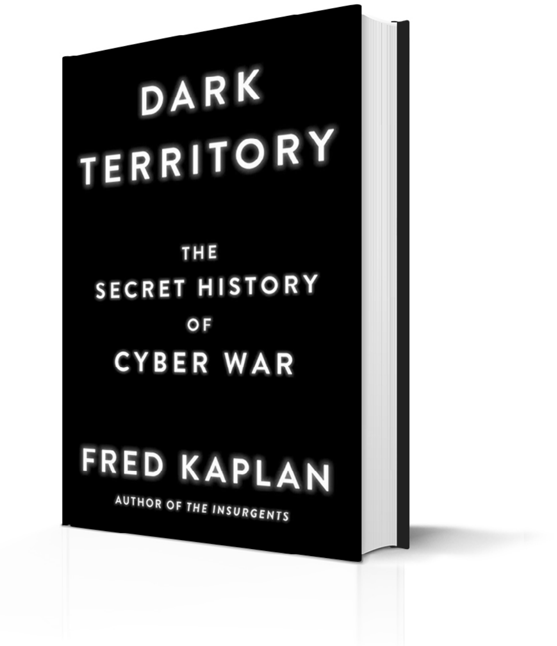
[22] The White House, *National Security Strategy* 27 (2010), https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf; Department of Defense, *Strategy for Operating in Cyberspace* (2011), http://www.defense.gov/news/d20110714cyber.pdf; Government of Canada, Canada's Cyber Security Strategy (2010), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx; HM Government, *The UK Cyber Strategy: Protecting and Promoting the UK in a Digitized World* (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

The Cyber Defense Review

◆ Book Review ◆

Dark Territory: The Secret History of Cyber War by Fred Kaplan

Reviewed by Dr. David V. Gioe



Writing a history of anything without clear or accepted chronological boundaries, such as cyber war, is a challenging undertaking. Even with a definite start and stop points, Winston Churchill still felt that he needed six enormous volumes, eight years, and a team of contributing authors to tell his history of the easily demarcated Second World War. British wartime code-breaker turned Cambridge historian, F.H. "Harry" Hinsley, in some respects had a more modest task than Churchill—to write a history of World War II examining only the intelligence aspect. Like Churchill, however, Professor Hinsley found that he required several research and writing assistants, many years of work, and four volumes to tell his history of World War II secrets, not to mention the benefit of over a quarter century of time—much-needed hindsight and cooling off of intelligence sources and methods—to place intelligence and code-breaking operations into their wartime context. Even Hinsley's abridged version of *British Intelligence in the Second World War* (1993) spanned a dense 628 pages. Thus, broad histories are exceptionally challenging to write—much more so in their own time—and compounded by the fact that any "secret history" is bound to be a historiographical challenge for even the most veteran researchers.

In *Dark Territory: The Secret History of Cyber War,* Fred Kaplan has undertaken this daunting task and produced a well-researched book with a lively narrative. Kaplan, the national security columnist for Slate, is no novice to writing on opaque subjects, especially ones still in the headlines and shrouded in governmental secrecy. His former works on a diverse range of topics from nuclear weapons to military operations demonstrate a malware-like ability to penetrate seemingly sealed systems which appears to offer nothing but a frustrating carapace to those that lack Kaplan's knack for investigative reporting. In some ways, Kaplan is the ideal author to attempt a secret history of cyber war: He is undaunted by technical complexity as evidenced not only by *Dark Territory,* but also his previous work on the nuclear arms race. Although technical enough to understand more than the basics of how cyber operations work, Kaplan keeps the narrative progressing and stays above the minutiae of coding and network integration. He never loses his intended generalist audience, and places cyber vulnerabilities into a larger political and international context. Kaplan reminds the reader that cyber operations are about technology and innovation, but equally, they're about people. It would be difficult to read *Dark Territory* and not find oneself rooting for Kaplan's protagonists—those cyber pioneers laboring in Pentagon basements, scientific labs, or at forgotten airbases, seeking to warn their Luddite leadership of danger ahead.

In the main, Kaplan adroitly navigates the problematic historiographical issues in intelligence history, relying overwhelmingly on off-the-record oral interviews, secondary sources and publicly available official policy announcements, directives, and strategies, such as those issued by the White House on certain national security topics. The closer Kaplan gets to present-day cyber operations, the more challenging reliable sourcing becomes due to classification issues (or some may say, "over-classification" issues). That Kaplan is forced to rely on interviews and anecdotes more than primary sources for his anecdotes and conclusions is yet another reminder of the challenges facing historians dealing with classified materials. The remedy, of course, is faster declassification review of relevant cyber-related materials, but that is a very long shot indeed. Edward Snowden likely felt this way, and thus took it upon himself to ensure that perhaps a million classified documents found their way into the public sphere through his devastating mass leaks, and historians are still grappling with the implications of mass leaks as primary source documents. Kaplan relies on remarkably little of Snowden's haul, perhaps because of their illegitimate provenance, but perhaps also because they lacked context, rendering them less reliable for authors.

The authoritative source material is a challenge for any secret history, and Kaplan's *Secret History* is no exception. Secret histories are often supplemented with oral interviews and secondary sources, but the best ones have primary sources at their core. Richard J. Aldrich's book, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* is the best example of primary source mastery which, instead of bogging it down, actually drives and enhances a narrative on technical topics such as signals intelligence and cyber history. This usually requires either a sizeable number of Freedom of Information Act requests (Kaplan cites a few), or tedious digging in the archives. Although written for a popular audience, Kaplan's work would have benefitted from further exploration of salient declassified primary sources, such as the National Security Agency's significant "United Kingdom—United States of America Agreement", the formerly highly classified secret treaty which governed signals intelligence (SIGINT) relationships between the US and the UK.[1] The UK-USA agreement is arguably the mustard seed of today's cyber operations, given that it is this agreement from 1946 (solidifying earlier wartime US-UK signals intelligence cooperation) that laid the groundwork for Anglo-American and "Five Eyes" partnership in cyberspace up to the present day. Given the enduring, secret—and occasionally controversial—reciprocal agreements between the NSA and Great Britain's Government Communications Headquarters (GCHQ), any history of cyber war could be given additional context and reliability with such newly accessible declassified source material.

The fact that a journalist of Kaplan's stature has logged into the cyber realm is itself a notable and promising development in cyber studies. To wit, no longer are cyber specialists the only ones with the technical credentials to write an authoritative book on cyber operations; non-specialist journalists, even a Pulitzer Prize winner such as Kaplan (who holds a Ph.D. from MIT in Political Science), are now interested in contributing to cyber studies as another window into international relations, national security studies, and organizational history, to name but a few. And in that sense, literature on cyber issues has become more relevant and accessible to humanities and social science generalists than ever before. This is a promising development for cyber studies in as much as cyber issues have successfully transitioned from specialist literature to a fair game topic for an author like Kaplan.

Kaplan's *Dark Territory* is far from comprehensive, but then a comprehensive cyber history is likely impossible, especially considering classification issues, but also given the blurred lines between code-breaking, communications and signals intelligence, electronic warfare, and even electronic or cyber operations enabled or supported by other intelligence types, such as Human Intelligence. Further, the geopolitical impact of these operations would take many more volumes to assess. As an example, Kim Zetter's *Countdown to Zero Day,* a single case study about the Stuxnet virus, is substantially longer and more detailed than Kaplan's *Dark Territory.* Therefore, Kaplan's book must be read as a complement or supplement to other works in the burgeoning cyber history canon, such as Jason Healey's *A Fierce Domain: Conflict in Cyber Space,* 1986-2012. As a historical primer on cyber operations, Kaplan's book does a great service opening other doors of intellectual inquiry regarding the relevance of cyber operations to current events, identifying the main actors and turning points, and critically, putting them in their own historical context.

Dark Territory: The Secret History of Cyber War by Fred Kaplan

Paperback edition of *Dark Territory,* with a new Afterword,
will be published in March 2017.

Author: Fred Kaplan
Publisher: Simon & Schuster, 2016
e-book: 353 pages
Language: English
ISBN: 978-1476763255

David V. Gioe is Assistant Professor of History at the United States Military Academy at West Point and History Fellow for the Army Cyber Institute. Dr. Gioe spent over a decade working in the U.S. intelligence community, both in the FBI National Security Division and in the CIA Counterterrorist Center (CTC). He retains his commission as a Naval Reserve Intelligence Officer. Dr. Goie earned his Ph.D. in Politics and International Studies at Corpus Christi College, University of Cambridge. He holds a BA in History and Social Science from Wheaton College, an MA from the Georgetown University School of Foreign Service, and is a graduate of the U.S. Naval War College Command and Staff program.

NOTES

[1] The National Archives (UK), Newly Released GCHQ Files: The UKUSA Agreement, http://www.nationalarchives.gov.uk/ukusa/, accessed 8 November 2016. See also https://www.nsa.gov/news-features/declassified-documents/ukusa/.

SUBMISSIONS FOR CDR ONLINE

The Cyber Defense Review (CDR) Online is designed for quick turnaround of original, unpublished work to facilitate authors quickly reaching the community of scholars, industry professionals, and military personnel with a stake in the cyber operations domain. If you agree to the provisions laid out in the following paragraph, please submit articles to cyberdefensereview@usma.edu. Be sure to include all elements listed in the checklist below.

VOLUME 2 • NUMBER 1 2017

THE CYBER DEFENSE REVIEW

Cyberspace in Multi-Domain Battle
Lieutenant General Paul M. Nakasone
Major Charlie Lewis

Clear Thinking About Protecting The Nation in the Cyber Domain	*General (Ret.) Keith B. Alexander* *Mr. Jamil N. Jaffer* *Ms. Jennifer S. Brunet*
Cybernomics – Changing the Economics of Cyber Defense	*Mr. Snehal Antani* *Mr. Ravi Iyer*
The Violence of Hacking: State Violence and Cyberspace	*Dr. Aaron F. Brantly*
Cyber (In)Security: Decision-Making Dynamics When Moving Out of Your Comfort Zone	*Mr. Andy Cohen*
Growing Role of Platforms in Cybersecurity	*Mr. Eric G. Troup*
INTRODUCTION *The Cyber Defense Review:* Rising Cyber Threat	Colonel Andrew O. Hall
BOOK REVIEW *Dark Territory: The Secret History of Cyber War* by Fred Kaplan	*Dr. David V. Gioe*

ARMY CYBER INSTITUTE • WEST POINT

SUBMISSIONS

1. We accept only complete, unclassified, ready-for-publication original works. We will screen them according to our editorial policy (provided below). We are committed to either publishing your work or returning with comment within two calendar weeks or possibly sooner.
2. We will make minor editorial corrections and formatting changes as we post works electronically. We are not staffed for extensive editing. Articles that require major editing will be returned to authors for correction.
3. Registered members of CDR Online community will be able to comment on journal entries. Comments will be moderated, however, be prepared for constructive criticism of your work.
4. We will always identify you as the author of your work and there is no profit made from publication.
5. Please review the editorial policy below for details regarding copyright and pre-publication review of your work.
6. If we decide to publish your work, you will be asked to complete and sign a Contributor Publishing Agreement. If you would like to review this agreement before submitting your manuscript, please contact cyberdefensereview@usma.edu.

Submission Checklist

When you submit, please be sure to include the following.

- ✓ Your work in Microsoft Word or rich text format (No PDF files).
- ✓ Your (and your coauthors) by-lines, email address, and a brief bio for each author. Three to four sentences is usually appropriate.
- ✓ Pictures and other graphics should be included in your document as you would like them to appear in the published article. Use of any graphics must comply with copyright provisions specified in the attached editorial policy.
- ✓ Articles for our online offering should be 1,500 – 4,000 words and include a 200-word abstract.
- ✓ Articles should be fully cited using the Chicago Manual of Style, 16th Edition.

Editorial Policy

The CDR accepts articles from across the spectrum of stakeholders in cyber operations to capture thoughts, ideas, and attitudes from beyond the Department of Defense (DoD) cyber community. We desire input from academia, industry, and government stakeholders, all of whom have a keen interest in our way forward in the cyberspace domain. Since cyberspace is global, we welcome and encourage international participation.

Submissions to the CDR will be screened by members of the editorial board to ensure they meet the following criteria. Articles should be:

- Relevant and timely; applicable to the broad cyber operations community.
- Complete and well-written, such that relevant content is clear and understandable.
- Sufficiently researched and well documented with a clear distinction between previous work and the authors' contributions.
- Free of significant grammar, spelling, or punctuation errors—otherwise work will be returned to the author for correction and resubmission.
- In compliance with copyright and pre-publication clearance review stated in the following paragraphs.

COPYRIGHT

Copyright law and the proliferation of methods used to disseminate art, illustrations, and photographs without attribution require the CDR to require the identification of all owners of any copyright-protected material. An author's reliance on fair use of copyright-protected material (including, but not limited to, direct text, tables, charts, maps, illustrations, graphics, and other visual material) is a subjective determination that cannot be made by the CDR.

If an author has developed a manuscript with co-authors, as a condition of employment, or pursuant to a contract (*work for hire*), the author may not be the sole copyright owner. The author is responsible for providing consent to use copyright-protected material with submitted manuscripts.

Authors must guarantee that manuscripts are their original work, necessary permissions for reproduction (if any) are provided to the CDR, and manuscripts do not contain any violations of copyright protection or otherwise infringe upon the rights of others.

As an official DoD publication, the CDR is not copyright-protected. However, the author retains all copy rights (as provided by 17 USC §501) in published manuscripts. The CDR does not manage copyright permissions for an author's work. Persons requesting permission to use copyright-protected material must contact the author directly.

In consideration for publication in the CDR, the author grants the DoD including all official activities thereof, the right to reproduce and use the article for training and other official purposes.

REVIEW & CLEARANCE

The CDR functions under the public affairs principle of *security review at source.* It is the author's responsibility to ensure that submitted manuscripts receive proper security review prior to submission. Manuscripts that are not characterized as opinion or historical pieces, or do not discuss or entail specific current capabilities or tactics, techniques, or procedures of military units and organizations do not require proof of security review. All other manuscripts must include such proof, signed by the security officer and public affairs officer of the author's assigned organization.

EDITORIAL PREROGATIVE

The CDR considers a manuscript's substantive accuracy, comprehensiveness, organization, clarity, timeliness, originality, and value to the cyber community in determining whether to publish an article, opinion, or review.

In the interest of clarity, brevity, accuracy, grammar, word usage, conformity style, presentation, and security, the CDR reserves the right to make minor editorial corrections and formatting changes. Any resulting changes to content will be provided to the author for approval prior to publication; articles that require major editing will be returned to the author for correction.

DISCLAIMER

The CDR does not screen articles to fit a particular editorial agenda, nor endorse or advocate material that is published. In fact, the Joint Ethics Regulation prohibits such endorsement. Rather, the CDR provides a forum for professionals to share opinions and cultivate ideas. Registered readers will be able to comment on published material to further expand the dialog. Comments will be moderated before posting to ensure logical, professional, and courteous application to article content.

Papers submitted for online publication should be between 1,500 – 4,000 words in length, with an abstract (roughly 200 words), introduction, body, and conclusion. References will be provided as endnotes and will be fully cited using the Chicago Manual of Style, 16th Edition format (http://www.chicagomanualofstyle.org/). Be sure to include author names, source titles, publishers, dates, journal volumes and numbers, URLs for online content, and page numbers.

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