VOLUME 1 ◆ NUMBER 2 FALL 2016

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 in the winter, spring, summer, and fall 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.

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

∞ *Printed on Acid Free paper.*

THE CYBER DEFENSE REVIEW VOL.1 ◇ NO.2 ◇ FALL 2016

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

BOOK REVIEW

The Cyber Defense Review

◈ Introduction ◈

VOLUME 1 • NUMBER 2 • FALL

The Cyber Defense Review: Discussions from the Front Lines of the Cyber Domain

Colonel Andrew O. Hall

VOLUME 1 • NUMBER 2

FALL 2016

THE CYBER DEFENSE REVIEW

Attacking Cyber: Increasing Resilience and Protecting Mission Essential Capabilities in Cyberspace
Lieutenant General Larry Wyche
Dr. Dawn Dunkerley Goss

Special Operations Forces Truths – Cyber Truths
Major General Stephen G. Fogarty
Major Jamie O. Nasi

Four Imperatives for Cybersecurity Success in the Digital Age: We Must Flip the Scales — *Maj. Gen. John Davis, USA, Ret*

Preparing for a Bad Day – The importance of public-private partnerships in keeping our institutions safe and secure — *Mr. Thomas J. Harrington*

Cyber Education via Mathematical Education — *Professor Chris Arney*, *Major Natalie Vanatta*, *Major Thomas Nelson*

Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex — *Dr. Mark Raymond*

INTRODUCTION
Discussions from the Front Lines of the Cyber Domain — *Colonel Andrew O. Hall*

BOOK REVIEW
Cyber War by Richard A. Clarke and Robert K. Knake — *Professor Chris Arney*, *Second Lieutenant Joseph Kozlak*

ARMY CYBER INSTITUTE • WEST POINT

INTRODUCTION

In our second edition of *The Cyber Defense Review (CDR)*, you will find opinions and insights from some of the most recognized innovators and leaders in the cyber enterprise on a variety of topics related to the ingenuity prevalent in today's military, the financial community, industry, and academia. Together, these authors offer their assessments and provide us with insights regarding the future of cyber conflict, current technical challenges and military requirements, and the potential for new public-private partnerships, educational constructs, and policy initiatives. Every article in this journal is intended to spur further thought and encourage debate on issues this cyber community grapples with every day. It is essential we understand the complex nature of our business and recognize opposing viewpoints on contentious issues.

Leading off the *Senior Military Leader Perspective* section, Lieutenant General Larry Wyche, Deputy Commanding General of U.S. Army Material Command, and Dr. Dawn Dunkerley Goss, relay their cyber technology and acquisition strategy to confront an evolving threat environment. Our Army Cyber Center of Excellence Commander, Major General Stephen G. Fogarty, and Major Jamie Nasi, provide an insightful article that gives the lineage of the Special Operations Forces Truths and illustrates their cyberspace domain relevance to advocate for the incorporation of a set of Cyber Effects Truths for the Army's contribution to the Joint Cyber Mission Force (CMF).

Colonel Andy 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 MNC-I/XVIIIth ABC Staff deployed to Iraq. He is a Cyber officer and was instrumental in creating the Army's newest branch.

In the *Professional Commentary* section, Major General John Davis (USA, Ret) of Palo Alto Networks, addresses the need to protect our information and networks. Recognizing the escalating threat to the military, civil, and commercial cyberspace environment, he socializes an initiative to return the advantage in the cybersecurity race to the defenders rather than the attackers through "Flipping the Scales." Next, in his article "Preparing for a Bad Day," Thomas J. Harrington, Citi's Chief Information Security Officer, reminds us that public-private partnerships build upon our arsenal of cyber capabilities and resources. By applying our resources, internally and through our external partnerships, we can develop an intelligence-led approach to predict, prevent, and successfully respond to cyberattacks.

Our *Research* section provides five remarkable and compelling articles on cyber education, cyber strategy and policy, and new cyber capabilities, techniques, and technological developments that highlight the importance and complexity of the cyberspace domain. In the first article, Professor Chris Arney, Major Natalie Vanatta, and Major Thomas Nelson provide a stimulating review of the United States Military Academy Math Department curriculum and demonstrate the importance of mathematics to the development of a robust cyber education. Next, Dr. Rosemary Burk and Dr. Jan Kallberg's provocative article claims that unilaterally not striking back against a cyber attacker can strategically create decisive capability and provide vital information for the refinement and evolution of the targeted state. Third, Colonel Pat Duggan asserts that the dynamic nature of cyber will be utilized by Special Operations Forces to support and shape national security.

Then, Dr. Mark Raymond offers you a deeper look

Secretary of Homeland Security Jeh Johnson and the Director of the ACI Colonel Andrew Hall at the Joint Service Academy Cyber Security Summit held at West Point in April of 2016.

into the complexity of cybersecurity policy. He challenges security and intelligence practitioners to think beyond the accepted definitions and carefully crafted scenarios to answer questions from the developing cyber regime. The *Research* section concludes with Dr. Paulo Shakarian and his world class research team at Arizona State University taking readers into the Darknet hacker communities and forums for an intense look at this rich source of cyber threat intelligence for security analysts. They introduce a game-theoretic framework designed to leverage the exploit data mined from the Darknet to provide system-specific policy recommendations. The data collection demonstrates how these communities leverage for valuable cyber threat intelligence, which highlights the lifecycle of vulnerability from identification to exploitation. We conclude this quarter's volume with a superb book review by Professor Chris Arney and Second Lieutenant Joseph Kozlak, on Richard A. Clarke and Robert K. Knake's important monograph, *Cyber War.*

These articles, commentaries, and reviews represent the dialogue we strive to foster in this journal, and our continuing promise to facilitate the intellectual debate surrounding our Nation's cyber mission. As you read this edition of the *CDR*, we invite you to consider your viewpoints on today's cyber challenges, and encourage you to reflect on how your contributions to this dynamic field can enhance our ability to provide the necessary cyber support to the Nation. Your fresh and innovative ideas are critical to our ability to remain the world's premier fighting force.

We have compiled an impressive list of authors for our winter issue, to include Major General Paul Nakasone, Cyber National Mission Force Commander, Mr. Eric Troup, CTO, Microsoft WW Communications and Media Industries, Dr. Baruch Fischhoff, Howard Heinz University Professor, Social Sciences and Decision Sciences and Engineering and Public Policy, Carnegie Mellon University, Colonel Mary Lou Hall, Center for International Relations and Politics, Carnegie Mellon University, and Dr. John Healy, Dr. Leland McInnes, and Dr. Colin Weir from the Tutte Institute for Mathematics and Computing.

The Army Cyber Institute is proud to bring you this discussion from the front lines of the cyber domain in both digital and print mediums. We encourage you to join the conversation through our online blogs, articles, and commentary at www.cyberdefensereview.org.

The Cyber Defense Review

◆ SENIOR LEADER PERSPECTIVE ◆

Attacking Cyber: Increasing resilience and protecting mission essential capabilities in cyberspace

Lieutenant General Larry Wyche
Dr. Dawn Dunkerley Goss

We are entering a new era of evolving threats, advancing technologies, and reduced resources. Adversaries continue to exploit weaknesses within interconnected systems, such as the Enterprise Resource Planning solutions that now power the Army's daily operations through the aggregation and analysis of vast amounts of data, sometimes from dozens of sources. Each of these sources brings its own level of threat and vulnerability, leading to an incredibly complex environment ripe for exploitation. Despite these challenges, Army Materiel Command (AMC) is employing an aggressive cyber strategy to ensure our resilience within an increasingly congested and contested domain.

In our growing, sophisticated, and evolving cyber threat environment, we have a particularly complex operational environment based on the global range of our missions coupled with the composite of public and private infrastructure storing and transmitting government and partner data; for example, over ten thousand suppliers support the Organic Industrial Base (OIB) alone. From the research and development of cutting-edge materiel solutions to the ongoing Retrograde from Afghanistan, our competencies are facilitated through the use of Information Systems and platforms that are often not under AMC control, sending information across networks that are compromised. This requires us to understand and manage the underlying supply chain, gain the ability to recognize attacks or intrusions when they occur, take immediate steps to mitigate these attacks, and then execute alternate processes as required, as real-time as possible, in order to complete the mission.

Recent events within the cyberspace domain have brought attention to the fact that we must take aggressive steps to better protect our essential data. The AMC Commanding General recently approved a ***Cyber Mission Assurance Plan*** to provide a supporting roadmap to be resilient during a time where all our critical functions rely on networks and access to information. In this plan, well-defined Lines of Effort assign responsibility

Lieutenant General Larry Wyche is the Deputy Commanding General of the U.S. Army Materiel Command, one of the Army's largest commands with 64,000 employees impacting 50 states and 145 countries. He also serves as the Senior Commander of Redstone Arsenal. He began his career in the enlisted ranks and achieved the rank of sergeant while serving as a Calvary Scout leader. He previously served as the Commanding General of the U.S. Army Combined Arms Support Command (CASCOM) and the Sustainment Center of Excellence at Fort Lee, VA. His previous assignments included Deputy Chief of Staff, 3/4, U.S. Army Materiel Command, and the Commanding General of the Joint Munitions and Lethality Life Cycle Management Command/Joint Munitions Command.

Lieutenant General Wyche received his commission as a Quartermaster officer from Texas A&M University, Corpus Christi ROTC, and graduated in 1983 earning a Bachelor of Business Administration. He earned master's degrees in Logistics Management from the Florida Institute of Technology and National Resource Strategy from the Industrial College of the Armed Forces.

within the command and establishes the required objectives and milestones to achieve the desired end state—that we have trusted and resilient infrastructures, systems, platforms, and processes that assure mission performance through improved cybersecurity, increased protection of cyber key terrain and information, strengthened network defenses, and a trained and aware workforce that implements best cyber practices from both government and industry. These objectives are then tracked, along their critical path of implementation, via the use of metrics assessing both the success of implementation and the level of positive effect on the command's cybersecurity posture.

A *Test-Assess-Revise* methodology is required, given the rapid evolution of cyber threats, cyberspace doctrine, and the network environment. As the threats are already so active and are growing, we cannot wait to start these activities until we have the 'perfect' solution. However, given the austere resource environment and the unknown effectiveness and efficiency of some of the proposed actions, we are testing and assessing high payoff and low resource cost activities. We have focused on those activities that increase resilience and are effective, sustainable, and efficient: improved internal and external information sharing, promoting cultural change across the workforce, and pursuing team oriented solutions leveraging the best of public and private cyber expertise.

The key to success is improved internal information sharing and collaboration across all stakeholders. We actively engage with the Department of the Army Staff, Army Cyber Command (ARCYBER), and supported and subordinate commands to ensure cohesive, unified action, and to maintain mission assurance and the freedom to operate across the entire enterprise. Enabling greater mission

Dr. Dawn Dunkerley Goss is the Chief of the Cyber Division, AMC G-3/4. Her team is responsible for AMC's operationalization of cyberspace to achieve the AMC commander's objectives, facilitate mission command, and maintain AMC's ability to *develop, deliver and sustain* in support of current and future Army and Joint missions.

Dr. Dunkerley Goss received a Ph.D. in Information Systems from Nova Southeastern University in 2011 with a doctoral focus of information security success within organizations. Her research interests include cyberwarfare, cybersecurity, and the success and measurement of organizational cybersecurity initiatives. She holds a number of professional certifications, including Certified Information Systems Security Professional (CISSP), Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), Information Systems Security Management Professional (ISSMP), Certified Secure Software Lifecycle Professional (CSSLP), and Certified in Risk and Information Systems Control (CRISC).

command and developing cyber resilience across AMC, specifically within the AMC workforce, facilitates our ability to operate and defend our cyberspace terrain. Legacy processes, methods, and cultural paradigms must yield to a new concept that cyberspace is an operational domain with a continuously changing and contested terrain. All operations have risk—it cannot be eliminated, so that risk must be understood and managed actively. We will never 'graduate' from this challenge, and can never stop in our efforts to improve our cyber resilience.

To meet the challenges of the contested cyberspace environment, a cultural change in the workforce is required to promote all IT users and professionals using best practices in cyberspace in order to operate in a manner that promotes, not hinders, our cyber resilience. The workforce is transforming the way it thinks about cybersecurity. As we continue to train, organize, and equip to take full advantage of cyberspace's potential, we are recognizing that adversaries want to undermine our ability to operate freely within this domain. Every time we enter cyberspace, regardless of where we are, recognizing we are in a contested environment is a fundamental requirement. Anticipating threat attempts to disrupt us, and consider the effects of an adversary's potential ability to destroy friendly networks should be a standard procedure. The protection of information and ability to guarantee its transport through cyberspace will be essential to our operations. Increasing cyber resilience is an imperative at all levels (User, System Administrator, system, network, etc.), as well as additional integration of cyber into all missions to leverage the opportunities of cyberspace and ensure that we maintain the future advantage over our adversaries.

Employing a logistics and sustainment enterprise-level cyber strategy is a total team effort and requires active participation from all stakeholders, and more broadly across the acquisition community. Both effectiveness and efficiency must be considered within the equation, as well as partnerships with organizations in academia, government, and industry to identify and solve long-term challenges, develop capabilities and capacity for the future, and recruit and retain the best cyber experts.

> All operations have risk—it cannot be eliminated, so that risk must be understood and managed actively.

We are the Army's subject matter experts on Materiel Development and Sustainment and will meet the challenge of maintaining our freedom to operate in cyberspace by leveraging the cyber experts and technology needed to execute our mission.

This plan towards resilience in cyberspace has already helped AMC increase our emphasis on cybersecurity and pursue our vision of being ***The Premier Provider of Army and Joint Readiness to Sustain the Strength of the Nation.*** However, we have much more to do, both in assuring situational awareness and protecting our cyber terrain through innovative solutions in a time of fiscal constraint, remembering that brave Americans around the world continue to depend on us.

Special Operations Forces Truths – Cyber Truths

Major General Stephen G. Fogarty
Major Jamie O. Nasi

INTRODUCTION

The Special Operations Forces (SOF) Truths—humans are more important than hardware, quality is better than quantity, SOF cannot be mass produced, competent SOF cannot be created after emergencies occur, and most special operations require non-SOF assistance—have become tried-and-true guiding principles for the special operations community.[1] This article explains why and how the United States Army can repurpose SOF Truths to serve as guiding principles to recruit, resource, and train effective Cyber leaders, operators, organizations, and capabilities. This article provides the SOF Truths lineage and illustrates their relevance to the cyberspace domain so as to advocate for the incorporation of a set of Cyber Effects Truths for the Army's contribution to the Joint Cyber Mission Force (CMF).

SOF TRUTHS

The earliest known published work incorporating the SOF Truths is the 1987 publication titled *United States and Soviet Special Operations;* a report to Senate Armed Services Committee. The SOF truths appear in the document's forward signed by Earl D. Hutto—Chairman of the Special Operations Panel—which was ghost written by John M. Collins, Senior Specialist in National Defense and retired Army officer with limited firsthand Special Operations experience.[2][3] By 1988, Brigadier General (BG) Dave Baratto, Commanding General of the John F. Kennedy Special Warfare Center and School, was confronted with the process of codifying special operations' distinctive operational considerations as tenets, and with assimilating them across the military services. His staff added the tenets as truths to complement the newly created SOF imperatives.[4] The SOF imperatives and truths act like the two sides of a coin for recruiting/training and implementing special operations forces. The truths form the basis of how to recruit, resource, and train SOF Soldiers, whereas the imperatives

Major General Stephen G. Fogarty assumed duties as the Commanding General, U.S. Army Cyber Center of Excellence and Fort Gordon on September 8, 2014. A career Intelligence Officer, his assignments include Commanding General, US Army Intelligence and Security Command (INSCOM); CJ-2, International Security Assistance Force; J-2, U.S. Central Command; Director, Joint Intelligence Operations Center-Afghanistan; Commander, NSA Georgia and 116th MI Brigade; Director, Integrated Survey Program, USSOCOM; G2, 101st ABN Division (AASLT); S2, 75th Ranger Regiment and S2, 2nd Ranger Battalion.

MG Fogarty holds a Bachelor of Arts degree in History from North Georgia College. He is a graduate of the U.S. Army War College with a Master's of Science degree in Strategic Studies. He also holds a Master's of Science degree in Administration from Central Michigan University. His military education also includes the MI Officer Basic and Advanced Courses, and the U.S. Army Command and General Staff College.

provide the framework that Army SOF commanders apply to mission planning and execution.[5] BG Baratto's initiative is clearly tied to the Army Chief of Staff establishing a separate branch for Special Forces officers on April 9th, 1987, the activation of United States Special Operation Command (USSOCOM) on April 16th, 1987, and the SOF community's need to describe its unique competencies inward to the members of its ranks, and outward to the Army as a whole.[6]

By the early 1990s, USSOCOM—under the leadership of General Wayne Downing—had embraced the SOF truths, albeit the accepted list did not include the original fifth tenet; most special operations require non-SOF assistance.[7] USSOCOM retained the four SOF truths throughout the 1990s and into the new century as shown by General Peter Schoomaker's statement published in August 1999.

> You've got to select people with the highest likelihood of success. Then you've got to train, educate, and assess them constantly. You've got to keep upgrading the quality. We have a set of four SOF truths: Humans are more important than hardware. Quality is better than quantity. SOF cannot be mass produced. SOF cannot be created after a crisis occurs. These truths guide how we think about building our force. They're simple, and we repeat them over and over, and we make it every commander's responsibility to make sure that his people understand them.[8]

In 2010, the SOCOM Commander, Admiral Eric Olsen, reincorporated the fifth—so called—'lost' truth. His reasoning for the decision was to emphasize the importance and contributions that non-SOF personnel provides to SOF.[9] Additionally, he felt the fifth truth helped dispel any "...unrealistic ex-

Major Jamie O. Nasi is a Psychological Operations Officer assigned to the United States Army John F. Kennedy Special Warfare Center and School Fort Bragg, NC and leads the Special Operations Element at the Army Cyber Center of Excellence at Fort Gordon, GA. MAJ Nasi received his commission as an Armor Second Lieutenant through ROTC at Norwich University. His recent assignments include Secretary of the General Staff, Military Information Support Operations Command (Airborne); Commander, HHC, 4th Military Information Support Operations Group (Airborne); and Detachment Commander, Bravo Company, 6th Military Information Support Operation Battalion (Airborne). He has multiple operational deployments throughout East and West Africa. MAJ Nasi holds a Bachelor of Arts degree in Peace, War, and Diplomacy from Norwich University and a Master of Science Degree in Information Strategy and Political Warfare from the Naval Postgraduate School. His education includes the Armor Officer Basic Course, Maneuver Captain's Career Course, and Joint Professional Military Education Phase I credit through the Naval War College Monterey Program.

pectations as to the capabilities SOF brings to the fight." [10]

Today, the SOF truths are still an integral part of SOF as currently depicted in the United States Army Special Operations Command's (USASOC) ARSOF 2022; a document that provides not only the intellectual framework but also the foundational precepts to ensure SOF will succeed in the future operating environment. [11] A direct correlation is present between the SOF truths and USASOC's priorities outlined in ARSOF 2022; win the current fight, strengthen the global SOF network, further Army SOF/CF interdependence, and preserve the force. [12]

CYBER BRANCH

Until the Army established the Cyber branch in 2014, most cyber work was performed by Soldiers and civilians in the Military Intelligence Corps and Signal Corps. On 1 September, 2014 the Secretary of the Army and Chief of Staff of the Army established the Army's newest branch in recognition that the demands of the cyberspace domain required a dedicated professional cyber workforce to conduct cyber effects operations in support of Unified Land Operations. While slightly ahead of its time, this decision made the Army fully compliant with DoD Directive 8140.01 (Cyberspace Workforce Management) signed on 11 August 2015 that established the Cyberspace Effects Workforce (the authors shorten to simply Cyber Workforce for the remainder of this article) as one of the four personnel areas within the greater cyberspace workforce. The Cyber branch is not only the Army's newest branch, it is also the smallest making it vitally important that only the most talented individuals are selected for the branch. Establishing basic principles for organizing, selecting, training, and operating the Army's contribution to the Joint Cyber Mission

Force is critical, and although the Cyber branch's roots are principally Intelligence and Signal, its future development is likely to be more similar to Special Operations Forces. Therefore, it is appropriate to determine if the tenets used by SOF can be applied to the Army's portion of the Joint Cyberspace Effects Workforce.

Humans Are More Important Than Hardware

It has been a long-standing conviction in the SOF community that humans are more important than hardware. Highly skilled Soldiers with the proper training and direction can accomplish more than the most advanced equipment in the hands of less capable forces. This is because properly prepared Soldiers have the ability to think, learn, reason, and quickly adapt to changing conditions in a way that lesser trained forces, even if better equipped, cannot. For SOF, Soldiers are their center of gravity.[13] In this environment, advanced equipment and systems are simply tools that enable SOF personnel to accomplish their tasks. The same can be said for the growing Cyber Workforce where operational agility, adaptive thinking, and innovative leadership are cornerstones to operational effectiveness. It is important to understand that while advanced platforms and systems are essential enablers for SOF and the Cyber Workforce, the useful shelf life of any specific "cyber" tool or platform is likely to be short, while investment in talent acquisition and subsequent talent management of the Cyber Workforce will produce a long-term return on investment, both now and into the future. Adopting a strategy of equipping the man vs. manning the equipment is equally important for SOF and the Cyber Workforce. This is why it is imperative to invest in rigorous selection, education, and training for our Cyber Workforce so they are prepared to overmatch any current or future US adversaries in and through the cyberspace domain.

Humans Are More Important Than Technology

Quality Is Better Than Quantity.

SOF relies on small teams of highly trained specialized personnel to operate across a range of critical capabilities, surgical strike to unconventional warfare, and numerous types of operating environments, permissive to hostile. Due to these considerations, SOF cannot sacrifice standards to create a larger force as it would likely lose its decisive advantage over the enemy. The Cyber Workforce also functions in complex environments with a myriad of operational risks and opportunities. They conduct operations in peacetime as well as periods of active hostilities, and their actions have the potential to create tactical, operational, and strategic effects—amid the rapid rate the cyberspace domain changes; fueled by advancements in technology and the absence of physical borders. Our adversaries in this environment are technically savvy, highly motivated, adaptive, and persistent. Our Cyber Workforce must not only be technically and tactically superior, but must operate morally, ethically, and within the law of armed conflict and specified rules of engagement. The training, education, and ability to work as a highly functioning member of a team required to conduct successful operations in and through the cyberspace domain simply requires a level of talent possessed by only a few. To allow or to enable the Cyber Workforce to succeed in this environment requires intensive talent management, realistic education and training, and persistent operations.

Quality Is More Important Than Quantity

SOF Cannot Be Mass Produced.

It takes skill to recruit and select, and years to train SOF Soldiers. After initial assessment and qualification training, pipeline training for individual operators and teams may take years of additional education and training to meet stringent operational requirements. This is by no means a cookie cutter approach to training and education; flexibility is built into the system exposing SOF to diverse opportunities that forces innovation to continually incorporate lessons learned and advanced techniques into their highly specialized formations. SOF must continually evolve to decisively beat adaptive adversaries. Like SOF, an effective Cyber Mission Force requires specialized recruitment, selection, training and career management processes to effectively access talent, train and educate the individuals and teams and aggressively manage their development. The Cyber Workforce unique mission and operational environment demands its members embrace a life time of learning otherwise our adversaries will enjoy overmatch. Technology changes at a rapid pace and so must the capabilities and development of our Cyber Workforce. The training pipeline to develop a single interactive operator requires over two years of intense training and education to become a mission ready, productive member of a Cyber Mission team. Production of Fully Operationally Capable (FOC) Cyber Mission Force teams takes many years as proven by DoD's multi-year Cyber Mission Force build schedule. The capacity to surge and meet urgent mission requirements is very limited; therefore, careful thought must be given to future force manning, mission alignment, and skill development requirements. Failure to maintain appropriate capability and capacity will have severe consequences for SOF and the Army's contribution to the CMF.

> Today, the SOF truths are still an integral part of SOF as currently depicted in the United States Army Special Operations Command's (USASOC) ARSOF 2022.

Cyber Forces Cannot Be Mass Produced

Competent Special Operations Forces Cannot Be Created After Emergencies Occur.

It is imperative that SOF forces exist and train in peacetime and are not a byproduct of an emergency. While it takes significant time to train competent SOF operators, it requires even more time to develop cohesive teams able to consistently and successfully perform the missions in the environments previously discussed. Similarly, a competent Cyber Workforce cannot be created in a crisis for these same reasons. The capability to conduct synchronized and successful cyber effects and electronic warfare operations cannot be developed overnight. They are the result of realistic training exercises and actual online operations. Most importantly, the Cyber Workforce must maintain persistent contact with emerging technologies, threats, and adversaries. Easy access to a persistent training environment featuring robust cyber ranges and a thinking and capable opposing force equipped with the most current tools, techniques, and technologies is required to assure the Joint Cyber Mission Force can over match adversaries in the cyberspace domain. This level of expertise cannot be built quickly.

Competent Cyber Mission Forces Cannot Be Created After Emergencies Occur

Most SOF Activities Require Non-SOF Assistance.

It is remarkably uncommon for a SOF element to operate unilaterally without outside support. Although SOF are highly skilled and extraordinarily trained, to maximize effectiveness, they often require non-SOF subject matter experts and capabilities; intelligence, logistical, and interagency support are just a few of the various types of support SOF may require. Close relationships with interagency and multinational partners are often the key to successful SOF operations. This truth is also applicable to the Cyber Workforce, which is often dependent on Signal, Intelligence, Electronic Warfare, Fires, and Information Operations capabilities as well as interagency, multinational, and commercial partners. Critical to this process is changing the culture in the Army to encourage effective collaboration with all the stakeholders in the cyberspace domain. This places a high premium on the Cyber Workforce to establish collaboration mechanisms outside of the highly classified and compartmentalized environment when possible and to ensure that stakeholders are represented by appropriately cleared liaisons. It is essential that the Cyber Workforce develops a culture that mandates ruthless collaboration with partners in academia, industry, interagency, and internationally.

> The same can be said for the growing Cyber Workforce where operational agility, adaptive thinking, and innovative leadership are cornerstones to operational effectiveness.

Most Cyber Activities Require Non-Cyber Workforce Assistance

CONCLUSION

It is apparent the SOF Truths are in fact relevant to the Cyber Workforce, and with minor modification can form a useful set of tenets to better enable assessment, selection, and training of the Army's contribution to the Joint Cyber Mission Force. Although additional Cyber Workforce Truths may be identified in the future, the five listed below can be applied immediately by the Army's newest branch:

Humans are more important than technology,

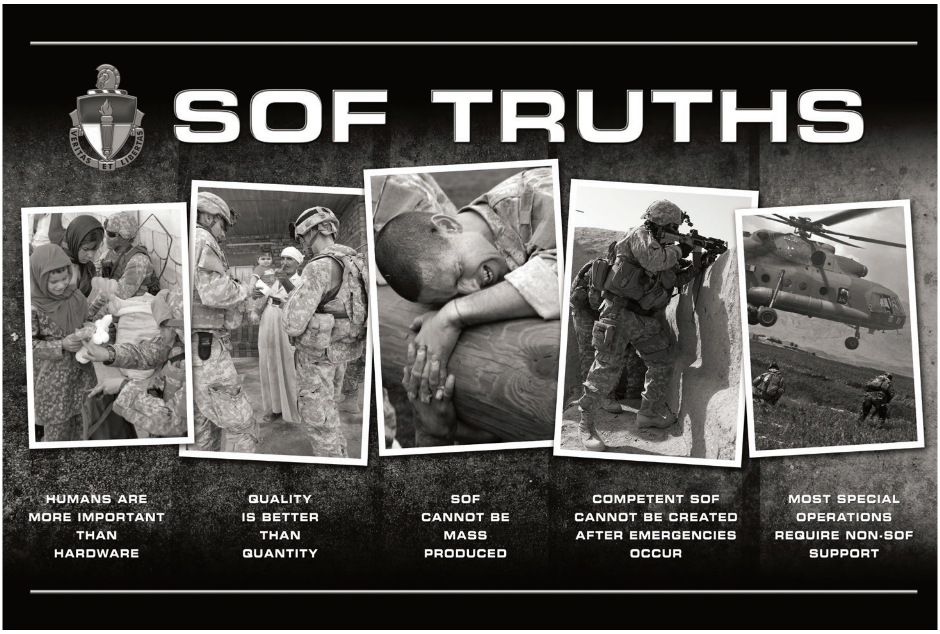
Quality is more important than quantity,

Cyber Forces personnel cannot be mass produced,

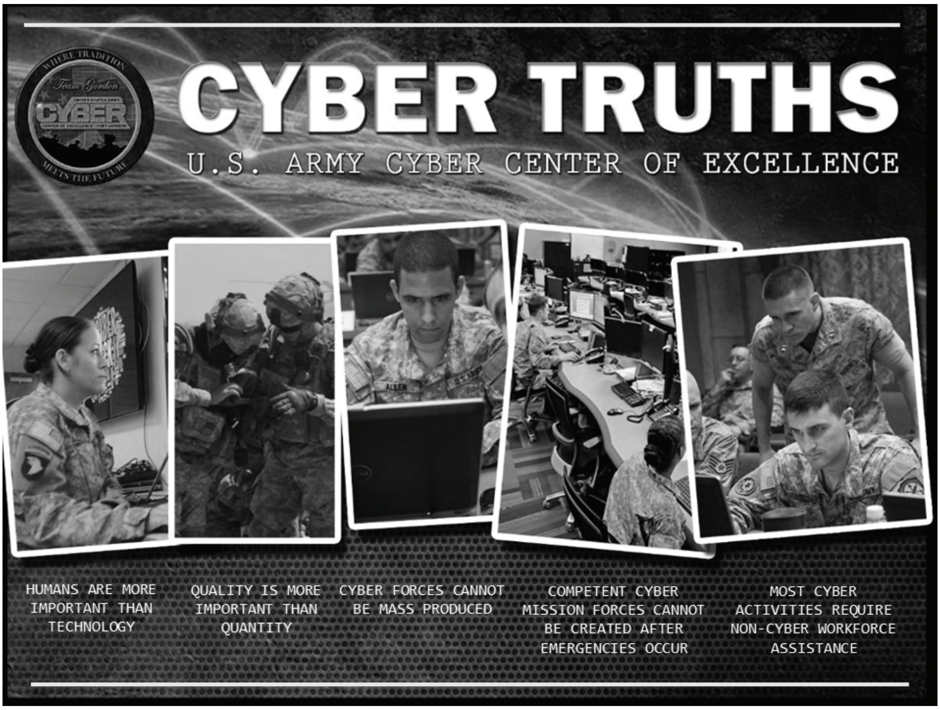
Competent Cyber Mission Forces cannot be created after emergencies occur,

Most cyber activities require non-Cyber Workforce assistance.

Predating the decision to form the Cyber branch, the Army transitioned the former Signal Center of Excellence at Fort Gordon, Georgia into the Cyber Center of Excellence or CCoE. The CCoE is the home of the Signal School and the newly formed Cyber School. The Cyber School is in the process of training and educating the officers, warrant officers, and noncommissioned officers who are the core of the new branch and the Cyber Workforce. Per Headquarters Department of the Army execution order 057-14, the CCoE is the Army's Force Modernization Proponent for Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, and Facilities (DOTMLPF) requirements, capabilities, and activities related to Cyberspace Operations, Signal/Communications Networks and Information Services, and Electronic Warfare. The Army Force Modernization Proponent System provides guidelines and functions for establishing and maintaining an effective force supporting Army warfighting requirements. As such, the CCoE is adopting the Cyber Truths as part of its strategy to educate, train, and develop current and future Cyber Workforce members to ensure their readiness to conduct cyber effects operations in support of Unified Land Operations.


SOF TRUTHS
VERITAS ET LIBERTAS
HUMANS ARE MORE IMPORTANT THAN HARDWARE
QUALITY IS BETTER THAN QUANTITY
SOF CANNOT BE MASS PRODUCED
COMPETENT SOF CANNOT BE CREATED AFTER EMERGENCIES OCCUR
MOST SPECIAL OPERATIONS REQUIRE NON-SOF SUPPORT

U.S. Army Special Operations Center of Excellence, U.S. Army Special Operations Center of Excellence Downloadable ARSOF Media, soc.mil, accessed April 14, 2016, http://www.soc.mil/SWCS/Posters.htm.


WHERE TRADITION MEETS THE FUTURE
Team Gordon
CYBER
CYBER TRUTHS
U.S. ARMY CYBER CENTER OF EXCELLENCE
HUMANS ARE MORE IMPORTANT THAN TECHNOLOGY
QUALITY IS MORE IMPORTANT THAN QUANTITY
CYBER FORCES CANNOT BE MASS PRODUCED
COMPETENT CYBER MISSION FORCES CANNOT BE CREATED AFTER EMERGENCIES OCCUR
MOST CYBER ACTIVITIES REQUIRE NON-CYBER WORKFORCE ASSISTANCE

NOTES

[1] United States Special Operation Command, *SOF Truths,* accessed March 30, 2016, http://www.socom.mil/pages/softruths.aspx.

[2] John Collins, "The Warlord on Special Operations Forces," *War on the Rocks,* September 10, 2013, accessed 30 March 2016, http://warontherocks.com/2013/09/warlord-on-special-operations-forces/.

[3] It is important to note that the SOF truths were likely articulated ideas already present within the ARSOF community prior to the publication's release date.

[4] Sean D. Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine,* Navyseals.com, accessed March 30, 2016, http://navyseals.com/nsw/adm-olsen-adds-lost-5th-sof-truth-doctrine/.

[5] U.S. Department of the Army, *ADRP 3-05 Special Operations,* (Washington DC: GPO, 2012).

[6] Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine.*

[7] Ibid.

[8] Eli Cohen and Noel Tichy, *Operation – Leadership,* fastcompany.com, accessed March 30, 2016, http://www.fastcompany.com/37511/operation-leadership.

[9] Naylor, *Adm Olsen Adds "Lost" 5th SOF Truth to Doctrine.*

[10] Ibid.

[11] U.S. Army Special Operations Command, "ARSOF 2022," *Special Warfare Magazine* 26, no. (2013): 9.

[12] Ibid.

[13] U.S. Army Special Operations Command, "ARSOF 2022," 18.

The Cyber Defense Review

◇ Professional Commentary ◇

Four Imperatives for Cybersecurity Success in the Digital Age: We Must Flip the Scales

Major General John Davis, USA, Ret

PART ONE OF A FOUR PART SERIES*

Having joined Palo Alto Networks following a 35-year career in the U.S. Army, the past decade of which I served in a variety of leadership positions in cyber operations, strategy and policy, I have found that many of the cybersecurity challenges we face from a national security perspective are the same in the broader international business world.

This article and the companion posts in The Cyber Defense Review Blog describe what I consider to be four major imperatives for cybersecurity success in the digital age, regardless of whether your organization is a part of the public or private sector.*

To provide a sense of what I intend to cover in this series, here are the major themes for each imperative:

- Imperative 1 – We Must Flip the Scales
- Imperative 2 – We Must Broaden Our Focus to Sharpen Our Actions
- Imperative 3 – We Must Change Our Approach
- Imperative 4 – We Must Work Together

ARTICLE 1 OF 4: IMPERATIVE 1: WE MUST FLIP THE SCALES

This first article in the series covers Imperative 1 for cybersecurity success in the digital age. Before I get to the details of the first imperative, allow me to provide some background and context for all four imperatives, and then I'll provide an executive summary of the first imperative.

Part Two, Three and Four of this series will be published on The Cyber Defense Review Blog at http://www.cyberdefensereview.org/blogs/.

Retired U.S. Army Major General John Davis is the Vice President and Federal Chief Security Officer for Palo Alto Networks, where he is responsible for expanding cybersecurity initiatives and global policy for the international public sector and assisting governments around the world to successfully prevent cyber breaches.

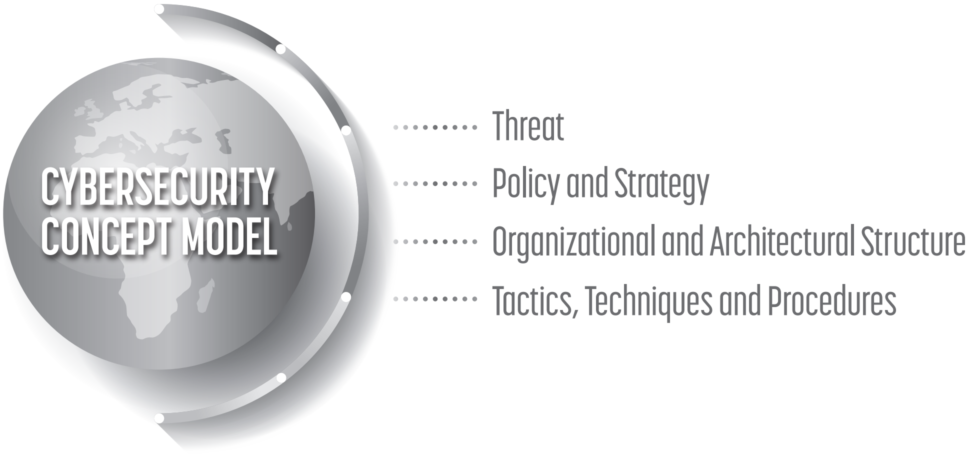
Prior to joining Palo Alto Networks, Major General Davis served as the Senior Military Advisor for Cyber to the Under Secretary of Defense for Policy and served as the Acting Deputy Assistant Secretary of Defense for Cyber Policy. Prior to this assignment, he served in multiple leadership positions in special operations, cyber, and information operations. His military decorations include the Defense Superior Service Medal, Legion of Merit, and the Bronze Star Medal.

Major General Davis earned a Master of Strategic Studies from the U.S. Army War College, Master of Military Art and Science from U.S. Army Command and General Staff College, and Bachelor of Science from U.S. Military Academy at West Point.

BACKGROUND AND CONTEXT

First, my role as the Federal CSO for Palo Alto Networks requires that I *evangelize* to the various groups of individuals, leaders, and organizations with which I interact. My job is to use my experience to ensure a deeper understanding of the cyberthreat landscape, and provide thought leadership about useful concepts to deal with a growing threat while ensuring that leaders can manage risk in ways that enable their business or mission.

Second, because of my military experience, I think of effective ***concepts*** regarding several key factors. I use these factors to explain concepts in a comprehensive way to describe each of the imperatives for cybersecurity success in the digital age. Figure 1 below provides the four factors that I use.



CYBERSECURITY CONCEPT MODEL
Threat
Policy and Strategy
Organizational and Architectural Structure
Tactics, Techniques and Procedures

THREAT
This factor describes how the evolving cyberthreat
and the response to those changes.

POLICY AND STRATEGY
Given our assessment of the overall environment, this factor describes what we should be doing, and our strategy to align means **(resources and capabilities–or the what)** and ways **(methods, priorities and operations–or the how)** to achieve ends **(goals and objectives–or the why).**

STRUCTURE
This factor includes both organizational (human dimension)
and architectural (technical dimension).

TACTICS, TECHNIQUES AND PROCEDURES (TTP)
This factor represents the tactical aspects of how we actually
implement change where the rubber meets the road.

Figure 1.

My last point of background and context is about the digital age, itself. So, what does the digital age environment look like? Two significant trends I would like to cover.

First, our growing societal reliance on technology for just about everything we do is only going to increase. This is not news to anyone; and, regardless of whether you are talking about public or private organizations or personal lives, there is no escaping the level of trust that we continue to place in technology. Equally increasing is the level of human connectivity, and in the devices we use to do almost everything in our daily lives. The phenomenon of the Internet of Things represents this trend.

The second trend is not news to anyone either. Just look at the growing list of headlines regarding cyber breaches across government and industry worldwide. Figure 2. depicts the most recent list of cyber breaches—it's a mess! I believe it's going to get worse before it gets better. You've all heard the tired (but, nonetheless, true) saying, "It's not a matter of if, but when." The trend is alarming; and, regardless of whether you sit in the public or private sector, you must recognize that the cyberthreat is a serious problem, representing an ***imperative for change*** if we are going to be able to continue to place trust in the opportunity the digital age promises.

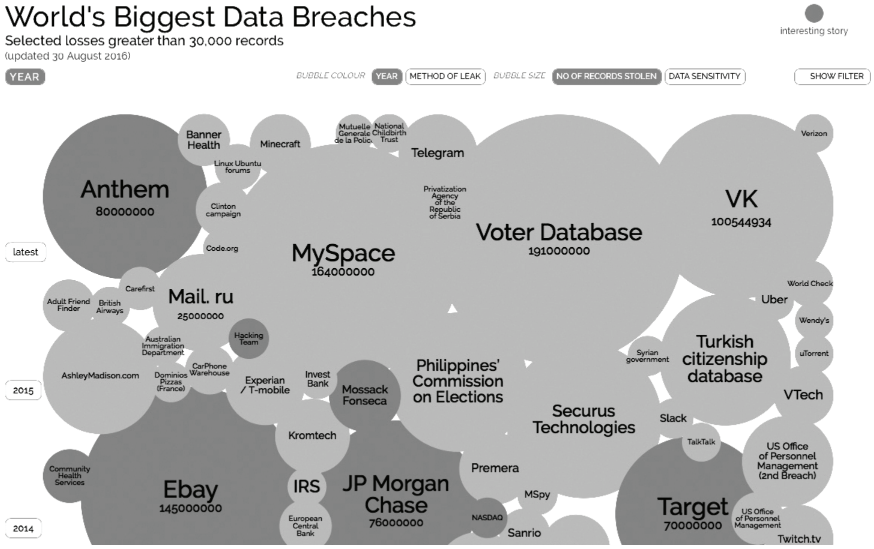


Figure 2. Source: http://www.informationisbeautiful.net

Using Figure 3. as a reference, we must *flip the scales,* or at least rebalance them, to improve the cybersecurity posture that we choose to live with today. Using the concept model below, I step through the implications via the categories of Threat, Policy and Strategy, Organizational and Architectural Structure, and finally Tactics, Techniques and Procedures (or TTP).

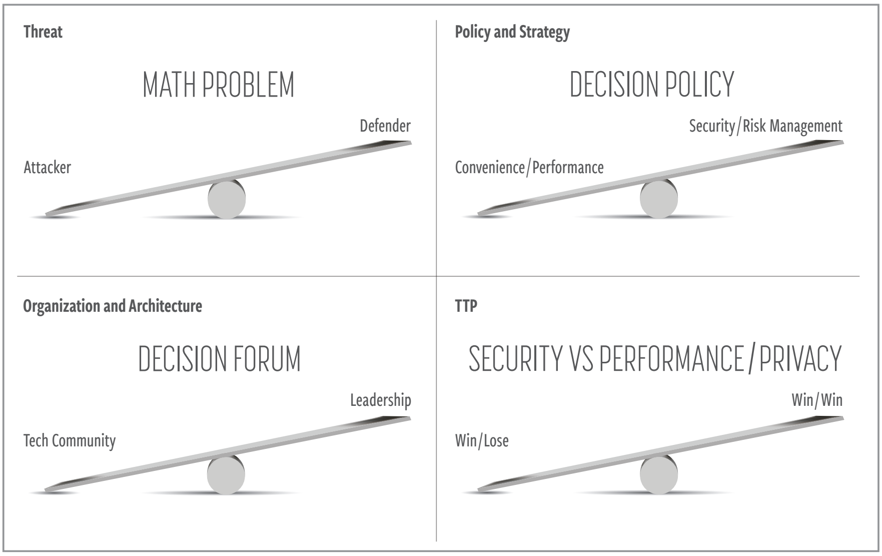


Figure 3.

EXECUTIVE SUMMARY

We have a math problem that is giving today's cyberthreats a significant advantage over our ability to secure and defend our networks. This issue pits a growing adversary marketplace—that leverages information sharing, automation and the cloud at increasing speed and decreasing costs—against the cybersecurity community, which is slow, clumsy, largely manual and increasingly expensive.

Part of the reason we have this math problem is due to legacy thinking and resulting policies that heavily favor opportunity and convenience over security and risk management rather than a more balanced approach toward both. Flipping the policy scale from a *trust everything* to a Zero Trust model ("never trust, always verify") will help to flip the scales on the attacker/defender math problem.

To change the policy balance and drive a real strategy that aligns limited resources and methods to achieve results also requires leaders to enter the decision-making forum for cybersecurity. A successful organization enables leadership to make decisions through collaboration between their IT and cybersecurity experts, working in tandem to provide precise, accurate and clear recommendations. This is how the leadership of an organization can drive successful policy and strategy. It is also how the leadership and tech teams should work toward common goals and routinely demonstrate progress with real, measurable results.

Finally, cybersecurity success in the digital age requires a new way of thinking about our TTP. Implementing real change needs rebalancing performance and security together, just as we also rebalance security and privacy together, empowering IT and cybersecurity teams to partner in a win-win dynamic, rather than pitting one community against the other with win-lose priorities. This is how an organization can go about safely enabling the high performance of its users, using the applications and content the organization requires to do its vital functions, including fixed, mobile and virtual capabilities throughout the organization's enterprise, from the cloud to the network to the endpoint device—BYOD or otherwise.

DETAILED DESCRIPTION OF IMPERATIVE 1

THREAT: Looking at this concept from a threat perspective, we all know that, today, the Attacker has a distinct advantage over the Defender. That's not news, and we all know that; but let's look at why that is true, and why cybersecurity will deteriorate unless we do something to *flip the scales*, or at least rebalance them toward a better security posture.

Our CEO at Palo Alto Networks, Mark McLaughlin, calls it a math problem. Due to the decreasing cost of automation and cloud-based capabilities, a growing marketplace of threat actor information sharing, and the ever-increasing attack surface with vulnerabilities growing in proportion due to the "Internet of Things" phenomenon, the Attacker's job is getting cheaper and easier every day. The Attacker only has to be successful once to get into your network and accomplish their nefarious objectives.

On the other hand, the Defender has to be everywhere, all the time. Additionally, the Defender, who typically uses manual procedures to respond, does not usually detect the threat in their networks until months or even years have passed. The average detection time is more than six months according to most cyberthreat research and analysis. This is very costly in terms of time, manpower, technology, complexity, reputation, brand, and, of course, money.

To illustrate further, I would like to use a few numbers to tell a story about the world of protecting your business from cyberattacks and this math problem. These numbers from our Regional Chief Security Officer (CSO) for Europe and the Middle East, Greg Day. In 2015, the Application Usage Threat Report from Palo Alto Networks saw 675,000 distinct threats, across almost 3000 applications. These are frightening statistics. But what does this mean in real terms to your business, to your team, or to you personally? To get a feel for that kind of meaning, you need a context that's relevant to your environment, so let me give you another number—1.5 million.cAccording to analysts Frost and Sullivan, this will be the shortfall of cybersecurity professionals by 2020.

This demand outstripping supply is good news if you're a security professional looking for a job, but bad news if you are trying to recruit cybersecurity professionals into your organization or retain your existing workforce. Many organizations have a model that is becoming harder and harder to sustain in this global environment of more threats and less security staff at the ready.

Implementing real change requires rebalancing performance and security together.

Who are these Defenders? The Chief Information Security Officer (CISO) and other IT security professionals defend their organization—against what, though? Today, it's not just an attacker; it's a marketplace, and that means groups of people sharing best practices with each other. A few years ago various governments were investing huge amounts of resources in developing incredibly sophisticated attack approaches. Today, anyone can purchase the same attack kit online for a few dollars, complete with instructions, and a how-to-get-started video.

This is why it's getting easier for Attackers, because of their decreasing costs and the abundance of resources available to them. They only have to be successful once to win, but this is probably a tiny percentage of their attack attempts. Contrast that with the CISO, who has to defend 100 percent of the time successfully. Attackers are crowdsourcing, yet CISOs are on their own.

I will demonstrate in the following sections of the concept model, how many leaders and security professionals are taking action to alter their defensive model to take advantage of the valuable assets they already have in *flipping the scales* to give the Defender more of an advantage than they have today.

POLICY: The legacy view is that opportunity and convenience drive technology (which are built-in) while security and risk management chase from behind trying to catch up (and are, therefore, bolted-on afterward).

The environment, as shown in Figure 2 above and captured in daily headlines about the latest breaches, is changing this balance; but the change is slow and uneven. This shift is beginning to bring the scales in Figure 3 to a more responsible balance. This includes changing a *left side of the scale* assumption that you are safe, to a *right side of the scale* assumption that the threat is going to get in, if it has not already, resulting in the need for a Zero Trust environment.

Security leaders want to reduce the workload on their organization. Getting back to our earlier math problem, here's another number—65,000. This figure comes from Greg Day, and identifies some of the reasons the network defender's workload is so big. When the Internet was conceived, that was the number of ports of communication that people thought might be needed for all the different traffic and protocols. This provided lots of scope and scale for flexibility. Today, we use very few of these traditional ports. Most of the traffic consists of either email or web-based protocols; however, within these, there are now thousands of Internet applications, and each has its own sub-protocols. You can block all these ports; but, since almost all the traffic comes through these same few ports, you cannot just block them. Using traditional technology, you have to trust these ports or block out all the traffic needed to run your business.

The Attacker has to only be successful once to get into your network and accomplish their nefarious objectives.

This policy means that security professionals have to program their legacy firewalls to block traffic using rules that are based on where traffic is coming from, where it's going to, and what type of traffic. And, of course, your organization wants to do new things all the time, so the policies have to change frequently. Your starting position is to trust all the traffic going through these few ports. Then you have to block traffic using policies—lots of policies. Policies on top of policies. Rules on top of rules. It's very difficult to even understand what the policies and rules of the past accomplished, and if the new policies and rules conflict in any way. This approach is costly, labor-intensive, and ineffective because it's using this old frame of reference that only adds complexity and cost to the equation, neither of which are your friends as a cybersecurity professional.

The only correction is to design a totally new type of technology using a different frame of reference based on how we use the Internet today. You need technology that understands modern Internet usage and identifies each of the applications that effectively uses its own protocols over the few trusted ports each business has enabled today. This is exactly why our tech industry is engineering next-generation firewalls to safely enable the applications and content required by an organization's users, whether fixed, mobile or virtual, to do the vital functions required for the mission or business.

The balance on the right side of the policy scale is called a Zero Trust model. Trust nothing unless it is defined as part of how you operate your business. This essential capability is unique. It also allows you to create rules that determine what traffic can flow into your organization. But, instead of being based on the port, the type of traffic, where it's from, and where it's going to, it's based on who wants to communicate, and what they want to do. That means the applications and content they want to use.

The result is that it's easy to define your company's way of doing business because of fewer policies, which are relevant to how your organization operates. They also make sense, and you can see your security policy written in black and white. It's more effective because your starting point is Zero Trust rather than trust everything, and it understands the sub-protocols that modern web applications use. It's easy to follow and much less work.

ORGANIZATION: The decision-making forum when it comes to dealing with cyberthreats has traditionally been within the technical (CIO/CISO/CSO) community, but the exploding threat challenge along with the changing balance between opportunity/convenience and risk are driving the decision-making forums into C-Suites and boardrooms; no longer the sole purview of the IT community. This is becoming more and more a leadership issue rather than just a technical concern. So this scale has already begun to flip, and that's a good thing!

Leadership is the most critical aspect of this imperative to change the balance and create an environment where those in the business of driving cybersecurity within an organization can begin to acquire an advantage over the threat. Leadership from the top drives the prioritization of resources and assets, enables an effective strategy that aligns the ways and means to achieve real goals, and requires the team to routinely bring back results that can be measured in relationship to the bottom line, whether you are a business or a national security organization.

This changing balance within the decision-making forum in no way diminishes the role of the technical community in the overall decision process. The tech community must take greater care than ever before to educate their leadership in clear, accurate ways so that sound decision-making is the result. Not all senior executives have the technical background to readily comprehend the details required to address what can be a very mysterious and complex problem set. It's incumbent on the leader's technical experts to explain issues in plain English to the maximum extent possible.

The technology environment associated with cyberspace has some of the most significant distinctions when compared to the traditional physical 'domains.' Scale, speed, and complexity (especially given the blurring of lines between human interaction with cyberspace and the various layers of technical, logical, physical and geographic segments) make analogies dangerous because, inevitably, the analogy falls apart at some point, and senior executives who think they understand what decision to make based on an imprecise analogy can be making serious mistakes.

TTP: So why does it seem we continue to lose, and the problem is deteriorating and not improving? Why haven't we all had a *Cyber Pearl Harbor* or *Cyber 9/11* epiphany? From what I can see, it's because there is still a false narrative about the balance between security and performance; that you can only increase one at the expense of the other. This traditionally describes a win-lose dynamic. In the world of business just as in the world of national and economic security, performance always wins, which is why most CISOs report to the Chief Information Officer (CIO). And when they do not, it's always a win-lose proposition pitting one community against another.

> This is why it's getting easier for Attackers, because of their decreasing costs and the abundance of resources available to them.

In this new environment, security and performance go hand-in-hand, so how do we enable a *win-win* dynamic? How do we put security into a model that safely and effectively *enables* performance, across all users, using all their applications, all their content, including mobile and virtual devices? Is that even possible? If your cybersecurity solution provider isn't working toward that objective, shouldn't they be?

In the above threat discussion, organizations are faced with the attacker having low costs and automation requirements, and the defender has high costs and humans performing manual tasks. This is why leaders are looking for another solution because this model is difficult to sustain. Perhaps it is even unsustainable.

Imagine if you could change the balance. At the moment, this precious resource—your staff—is focused primarily on discovery. Taking productive business action is secondary. This model gives a poor return. What if your people only took productive business action and the discovery part was automated? That model would give you a much higher return. More on manual vs. automated in one of my next *CDR* Blog posts about other imperatives for cybersecurity success in the digital age.

Helping us to pursue a win-win dynamic is to speak with more clarity and accuracy about what we are trying to do with information sharing to provide cybersecurity and distinguish that from some of today's conflated ideas about providing *traditional* security and the associated *surveillance* issues that get carelessly lumped into cybersecurity discussions.

In addition to the false narrative about performance vs. security, I think there's another false narrative regarding security vs. privacy. In the cybersecurity world, unlike the world of counterterrorism and surveillance issues, security ensures privacy; it doesn't detract from it! For example, we should begin to clearly identify exactly what kind of cyberthreat information needs to be shared, and how a narrow focus on that specific information has little (or maybe even nothing) to do with privacy-related information.

I will cover more about information sharing in Imperative 4; but, for now, let me summarize the key tenets of this first imperative about *flipping the scales.*

CONCLUSION

Cybersecurity success in the digital age requires immediate action to change several important dynamics that are currently out of balance. Legacy thinking and resulting policies put the cybersecurity community on the wrong side of a math problem when it comes to the threat, and in a win-lose dynamic with both the IT community and our leadership when it comes to choosing between performance and security. We have to *flip these scales,* with organizational leadership driving this effort accompanied by active IT participation, and cybersecurity communities working toward common goals.

We also need to start throwing the weight of our technology, processes, and people on the side of the scales, favoring next-generation technology that recognizes how the Internet works today, leverages the powerful advantage that automation brings to discovering threats on a wider scale, and in reduced time, and saves our most precious resource–our people–to do what only people can do instead of spending all of our resources in "cleanup on aisle 9" mode.

Next in the online *CDR,* our series continues with Imperative 2 for cybersecurity success in the digital age: ***We Must Broaden Our Focus in Order to Sharpen Our Actions.***

Preparing for a Bad Day – The importance of public-private partnerships in keeping our institutions safe and secure

Thomas J. Harrington

Today's cyber threat landscape is evolving at a rate that is extremely aggressive, and attacks are becoming more complex and targeted. Cyber criminals are growing increasingly more sophisticated and harder to predict, the number of connected devices is increasing exponentially, and the growing reliance on the cloud-based systems potentially opens up new attack surface for our cyber adversaries. These factors mean that today's defense techniques and strategies will need to evolve with the threat in order to keep our institutions and information safe and secure. In today's interconnected world, no single entity or organization has full visibility into the threats that exist, and the existence of partnerships, including between the public and private sectors, is extremely important and necessary in protecting us all. As a private institution, we recognize the need to, in a privacy protective manner, build strong relationships beginning with our internal teams and with our critical partners, such as government agencies, the military, and our business partners and clients, all working as a strong network to achieve the common goal of defending against bad cyber actors.

At Citi, our philosophy to keep our firm safe is built on investments in talent, teamwork, and technology. These pillars are critical in supporting our intelligence-led, threat-focused organization and helping us prepare for a *bad cyber day*. Talent management and development are extremely important when thinking about the future of an organization. Our financial community strives to recruit, hire, train, develop and retain talented colleagues to help give us any advantage possible to gain the high ground on the cyber battlefield. We are focused on transforming our workforce by investing in top-level cyber intelligence and Information Security talent from the private and public sectors, as well as from academic centers of excellence.

Thomas J. Harrington is Citi's Chief Information Security Officer. Tom retired with 27 years of law enforcement and national security experience. Mr. Harrington was the former Associate Deputy Director for the FBI and is a recognized leader in the global law enforcement and intelligence communities.

Our mission to recruit and retain top talent spans from recent college graduates with cutting edge training, to seasoned professionals from various backgrounds. These backgrounds include information technology specialists, information security specialists, intelligence analysts, communications specialists, and even those with political science backgrounds. Teamwork is a value that is essential for any organization regardless of size or function.

In an institution as widespread geographically as Citi, teamwork and the elimination of operating in silos is not just of high importance, but the protection of our assets depends on it. Each member of our team must recognize that the advanced adversaries are demonstrating growing sophistication, speed and responsiveness to our changing defense posture. These adversaries are well-networked and sharing knowledge and experiences at a rapid pace. We are focused on implementing leading management practices and initiatives to maximize collaboration, learning, and innovation across functional areas.

To be successful, each day we must demonstrate an ability to learn and share with a wide internal and external audience in a way that empowers them to act positively to safeguard our organization. We are also focused on deploying innovative technologies to secure the business and identifying disruptive technologies that enhance safety and security. We are developing information-sharing platforms, intelligence products, and operational playbooks that inform executive action and decision-making. Our ultimate goal is to evolve our information security programs real-time knowledge of threats and our posture against those threats—in order to prevent, detect, and when possible predict attacks, make risk decisions, optimize defense strategies, and enable action in response to those threats. Firms across industries, including financial services, must develop a successful battle rhythm focused on information security.

Critical to any organization that wants to achieve an upper hand in the cyber battlefield is the ability to attain what we and our military partners call *Situational Awareness* or commonly referred to as SA. In order to achieve a constant state of SA, Citi is taking steps to create a Cyber Common Operational Picture (COP). This will allow key leaders to have a real-time view of what is happening in the cyber realm, whether it's in the middle of a cyberattack or steady state operations, it is highly critical we maintain a holistic view of the cyber problem set.

Just as the military trains its forces to operate on battlefields against an asymmetric adversary, Citi depends on proper training and constantly exercising to ensure we build muscle memory into our own Standard Operating Procedures (SOPs) or playbooks. We recognize that having sophisticated technology and skilled talent is only half the battle with staying one step ahead of our adversaries. As a result, Citi has taken a proactive approach in achieving the other half by continuously and deliberately testing plans, validating capabilities, and identifying areas for improvement.

In today's interconnected world, no single entity or organization has full visibility into the threats that exist.

Ensuring a good defense is in place requires an organization in concert with one another, to incorporate several key elements when faced with an ever-evolving cyber adversary. Neither Citi nor any other organization can be prepared to defend itself without proper training and exercises. As with soldiers going into a combat zone, firms must train and exercise its cyber talent using a similar methodology used by the Department of Defense (DoD) and Department of Homeland Security (DHS)—*Train, Plan, Assess, Educate, Improve, and Train.* By employing this methodology, companies like Citi can conduct custom cyber-focused exercises that meet organizational objectives.

A key component of our exercise program is the *train up* piece—while not everyone at Citi has a key role or responsibility when it comes to a cyber crisis, it is important we constantly train our business staff to understand and provide a general understanding of Citi cyber capabilities and threats. Outside the mandatory annual information security training all employees must complete, our exercise team conducts *pre-exercise* training to exercise participants and observers. Doing this ensures that *non-cyber* functions and roles within Citi are afforded an opportunity to become familiar with *Cyber at Citi* and provides them an understanding of exercise expectations. As part of the exercise methodology, we then move into the Planning Phase, which is perhaps one of the most crucial elements.

Citi employs a core planning team concept when it comes to planning the exercise scenario. In order to make the exercise realistic, our team works with various internal partners to ensure the scenario is robust and realistic. Our end state goal is to make the exercise as immersive and real, as if participants were actually in the crisis real-time. This is done by creating real world exercise artifacts, such as news video clips, media reports, FBI and DHS reports, phone calls, emails, and social media postings. Over the last year, we have invested significant time and energy into building cyber incident response playbooks that serve as a baseline for notification authorities.

As with any plan or playbook, it has little to no value unless it is tested and exercised on a routine basis (scheduled or unannounced). Over the past few years, Citi has and continues to lean forward with setting the example by instituting a formal cyber exercise program. Not only have we started our own program, but we have also encouraged and assisted other banks and our clients to do the same. We know that building our internal capability and strengthening our cyber readiness posture is crucial to our individual success as a firm, but also recognize we—as an industry—must work together to ensure safety and security of the US financial ecosystem. Citi does this by consistently partnering with global government agencies, including domestically the U.S. Treasury, U.S. Cyber Command (USCYBERCOM), the Army Cyber Institute (ACI), the Naval War College, the DHS, the Federal Bureau of Investigation (FBI), and the Financial Services-Information Sharing Analysis Center (FS-ISAC), to plan and execute critical private-public sector information sharing cyber exercises.

To ensure the safety and security of our institution and industry, it's imperative for us to focus on becoming true learning organizations.

To ensure the safety and security of our institution and our industry, it is imperative for us to focus on becoming true learning organizations. We must prioritize the education and training of our employees and constantly transform andadapt to keep up with bad actors and emerging threats. All of Citi's training exercises are followed by After Action Reports and Improvement Plans that require actionable changes by our businesses.

While we stretch our imaginations to anticipate what our adversaries have in mind for their next attack, we can and will build upon our arsenal of cyber capabilities and resources. By applying our resources, internally and through our external partnerships, we can develop an intelligence-led approach to predict, prevent, and successfully respond to cyberattacks we may face. It is crucial that we continue to develop our staff to think *left of boom* to detect potential threats and properly respond in a timely fashion using documented and tested processes. We must also, in a privacy protective manner, continue to enhance our public-private sector information sharing mechanisms with our external partners like the military and US government agencies to ensure we all receive actionable and timely intelligence to make informed decisions and take appropriate actions. Most importantly, we must all be continuously learning and adapting our talent, tools, and technology to the ever-evolving cyber threat landscape.

This article reflects the views of the author and should not be viewed as representing the views of Citi nor the FBI. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

The Cyber Defense Review

◇ Research Articles ◇

Cyber Education via Mathematical Education

Professor Chris Arney
Major Natalie Vanatta
Major Thomas Nelson

ABSTRACT

Cyber is more than programming 1s and 0s, it is an interdisciplinary domain that involves elements of many disciplines of science, engineering, and humanities. Understanding mathematics is critical to understanding the cyber domain. At the United States Military Academy (USMA), the Mathematical Sciences Department is contributing to cadets' cyber education. The Military Academy CYBER Education Working Group produced initial thoughts on how to educate in this domain.[1] Using this construct, this article identifies the knowledge, skills, and attributes that are elements of USMA's core mathematics, network science minor, or mathematics major. The intent is to help prepare future military officers for leadership roles in the cyber-affected world in three tiers: (1) what all officers should know, (2) what highly technical officers should know, and (3) what cyber leaders should know.[2] All officers should have a broad professional cognizance of cyber operations, while highly technical officers and cyber leaders could benefit from a more in-depth understanding of mathematics relative to cyberspace.

INTRODUCTION

> *"If I were again beginning my studies, I would follow the advice of Plato and start with Mathematics."* – Galileo Galilei[3]

Jeff Immelt, Chairman of the Board and CEO of General Electric, recently reinforced Galileo's quote at *Business Insider's* IGNITION 2015 conference when he remarked that his most valuable qualification was his undergraduate mathematics degree. He said, "I use my math major every day—I don't use the MBA quite as much." He went on to say that running a company is about problem-solving. That's something he learned about in his undergraduate studies, due to "the inherent intellectual curiosity around

Brigadier General (Retired) Chris Arney is a Professor of Mathematics at the United States Military Academy and former Head of the Department of Mathematical Sciences. He holds a Ph.D. in Mathematics and M.S. Degrees in Computer Science and Mathematics from Rensselaer Polytechnic Institute. He also holds a B.S. in Engineering from the United States Military Academy. A career Military Intelligence officer, he has served in numerous tactical assignments, teaching assignments at USMA, NASA Langley Research Center, and the Army Research Office. His current research includes cooperative game theory, applications of network science, and mathematical applications to cyberspace.

Major Natalie Vanatta is a Cyber Officer currently serving as an Academy Professor with the Army Cyber Institute at West Point, NY. She has worked from the tactical to the operational level in the signal arena while also teaching/researching in the cyber field. She holds a Ph.D. in Applied Mathematics from the Naval Postgraduate School (NPS), an M.S. in Systems Engineering from NPS, an M.S. in Mathematics from Stevens Institute of Technology, and a B.E. in Computer Engineering from Stevens Institute of Technology. MAJ Vanatta has completed multiple tours in Operation Iraqi Freedom (OIF) and her research interests are in encryption, malware detection, active cyber defense, and human behavior.

Major Thomas Nelson is a Cyber Officer and currently the Operations Officer for the 782d Military Intelligence Battalion (Cyber) at Fort Gordon, GA. He most recently served as an Assistant Professor of Mathematics at the United States Military. He holds a M.S. degree in Applied Mathematics from the University of North Carolina-Chapel Hill, and a B.S. in Mechanical Engineering from the United States Military Academy. Commissioned in the Infantry, he served in numerous positions with the 82nd Airborne Division and 4th Infantry Division in Iraq and Afghanistan. His research interests include Computational Fluid Dynamics and Anomaly-Based Intrusion Detection Systems.

math and physics."[4] That same intellectual curiosity and problem solving is expected of all officers, particularly those entering the Cyber Mission Force (CMF).

At the United States Military Academy (USMA), the Department of Mathematical Sciences is contributing to cadets' cyber education. Cyber is more than programming 1s and 0s, it is an inter-disciplinary domain that involves elements of many disciplines of science, engineering, and humanities. Initial thoughts on how to educate in this domain were produced by the Military Academy CYBER Education Working Group.[5] Using their construct, this article identifies the knowledge, skills, and attributes that are elements of the core mathematics, network science minor, or mathematics/operations research majors at USMA. Ultimately, the intent is to help prepare future military officers for leadership roles in the cyber-affected world in three tiers: (1) what all officers should know, (2) what highly technical officers should know, and (3) what cyber leaders should know.[6] We believe all officers should have a broad professional cognizance of cyber operations, of which USMA's core mathematic program contributes. Highly technical officers will benefit from the math department's network science minor, and some cyber leaders would benefit from mathematical sciences major. Additionally, the military services provide numerous opportunities for graduate work in mathematics that contributes to the cyber domain.

> Two core objectives of the mathematics education at USMA is to acquire a body of knowledge, and to develop a fundamental understanding of the basic tenets of mathematics, science, and engineering.

WHAT ALL OFFICERS SHOULD KNOW: BROAD PROFESSIONAL COGNIZANCE OF CYBER OPERATIONS IN THE CORE MATHEMATICS PROGRAM

There are two terminal objectives of the core mathematics education at USMA: to acquire a body of knowledge, and to develop thought processes fundamental to understanding the basic tenets of mathematics, science, and engineering. A cadet's mathematical journey affords them opportunities to develop as life-long learners capable of formulating intelligent questions and researching answers independently and interactively. Central to the entire USMA program is the concept of problem-solving through modeling.[7] All cadets take a modeling course (MA103 or MA153), a calculus course (MA104 or MA255), and a statistics course (MA206). Officers in the Cyber Branch and those doing cyber-related work in other branches will be required to model and solve problems. Several lessons throughout the core mathematics program lend themselves to ensuring all officers have a basic understanding of the math behind cyber operations.

MATHEMATICAL MODELING (MA103)

This course emphasizes applied mathematics through modeling. Students develop effective strategies to solve complex and often ill-defined problems. The course exercises a wide array of mathematical concepts while nurturing creativity, critical thinking, and learning through activities performed in disciplinary and interdisciplinary settings. A block of the instruction in the course is on modeling with matrix algebra. In this block a lesson is taught on cryptology with all students taught the role of cryptology in military history and the basics of the encryption and decryption processes. Students use a transformation matrix for encryption and the inverse of the transformation for decryption. In this lesson students are taught, "the design of the encryption algorithm, and the mathematics required to support the decryption process is where the art and science of cryptology lies. Its sophistication ranges from simple procedures such as the matrix algebra presented in this section, to far more advanced techniques that leverage complex machines and the computational power of computers. Much like network science, the study of cryptology is extensive; entire courses, as well as entire careers of study and research, are dedicated to it."[8] In the lesson, students role play a WWII scenario encrypting and decrypting message intercepted from a German courier.

The mathematics modeling course also teaches two lessons on networks (one on network flow and the other on network centrality). The lesson on network flow discusses rules for network flow processes, applies the mathematics to military networks, and introduces problems to quantify the flow between nodes using linear algebra. The lesson on network centrality discusses the conception of social networks, internet structure and process, and how network analysis determines the most important node. Examples include Facebook and Google's page rank algorithm. This ensures all cadets receive a basic understanding of networks, network science, and the major domain and tools of cyberspace during the core mathematics curriculum.

SINGLE VARIABLE CALCULUS (MA104)

The goal of this course is to foster knowledge and understanding of single variable calculus, including the concept of the derivative and the integral, and to apply these concepts to model and solve problems, and to interpret and communicate the results in context. During the calculus applications block, the course covers several topics that are loosely related to cyber including rates of change in the natural and social sciences, exponential growth and decay, optimizations, Newton's method, applications to physics and engineering, and probability.

One lesson specifically addresses “applications to cyber operations.” This lesson gives the students a background on information theory and Claude Shannon’s interpretation of entropy. Students are given a scenario where they need to use integral calculus to determine the entropy of several different systems used in communications and secrecy systems. Using this information they communicate an argument as to which encryption algorithm a bank should use for their website. Students then learn about several government and military applications of cryptographic systems to include the one-time pad. This lesson and the other applications provide students a broad understanding of how math is used in the cyber domain.

PROBABILITY AND STATISTICS FOR ENGINEERING AND THE SCIENCES (MA206)

This course helps students use mathematics to model real-world variation and assess the likelihood of events. The course shows students to use statistical tools to help draw appropriate conclusions from data. It also teaches reliability analysis of independent systems with component diagrams and it works through reliability of systems/components in series and parallel. The current textbook example focuses on the reliability evaluation of solar photovoltaic arrays in series-parallel and total-cross-tied. Theses to arrays are set up very closely to the ring and mesh network topologies of computer networks. The same analysis on the solar arrays can be applied to predicting the system lifetime of computer networks.

The course then models uncertainty in the context of several different probability distributions—discrete and continuous. In this block, cadets execute a mini-project focused on the phases of network penetration. Cadets are required to program and conduct Monte Carlo Simulations on the probability of an attacker gaining access to the system within a certain timeframe and/or at a certain cost in resources. These are statistical simulations utilize sequences of random numbers to replicate real-world scenarios. Cadets not only build Monte Carlo simulations in Excel or R, but also interpret the results, and answer probability and analysis questions.[9] The statistical modeling in this course also gives cadets the ability to write, debug, and use a mathematical computer code to a real life scenario. Statistical and uncertainty models can be used to model other applications in the cyber domain.

Cyber is more than programming 1s and 0s, it’s an interdisciplinary domain that involves elements of science, engineering, and humanities.

NETWORKS FOR CYBER OPERATIONS (MA490)

Networks for Cyber Operations is a course intended to serve as an integrative experience for cadets of all majors and fields of study.[10] This course was formally known as Application Problems for Mathematics, Science, and Engineering. This specific offering of the course is new to academic year 2016 and focuses on networks for cyber operations. The seven-course blocks are as follows: Network Science, Cryptography, Cyber Mission Forces, Internet of Things, Social Sciences, Data Analytics and Science, and Tactical Cyber (Support to Corps and Below). The course enables students to confront cyberspace issues by modeling, solving, analyzing, and understanding problems involving cyber processes and structures on networks. The students learn about networks, perform complex modeling, work on a topic associated with this subject, write a book review, produce a poster, and give a presentation to the class.

All cadets taking the course complete a semester long project and presentation for USMA Projects Day in one of the following domains: Cyber and Social Movements, Cyber and Social Media, Security of the Internet, or Infrastructure Vulnerability. Although taught by USMA Department of Mathematical Sciences instructors, the course leverages the experience, knowledge, and expertise of the Army Cyber Institute (ACI), and other partner organizations (such as Combatting Terrorism Center, Department of Social Sciences, and FBI) for several guest lectures. The current section consists of 12 cadets (11 are math majors and one is a computer science major) that upon graduation will be commissioned into the Army's Cyber, Armor, Aviation, Military Intelligence, Air Defense Artillery, Field Artillery, Engineer and Infantry branches.

> Network Science is an inherently interdisciplinary academic field which studies complex networks such as telecommunications, computer, biological, cognitive, and social networks.

WHAT (SOME) HIGHLY TECHNICAL OFFICERS SHOULD KNOW: NETWORK SCIENCE MINOR

Network Science is an inherently interdisciplinary academic field which studies complex networks such as telecommunications, computer, biological, cognitive, and social networks. Network representations of these systems lead to predictive models and insights into how networks behave and evolve. Students who minor in Network Science graduate with an enriched understanding of the interrelationships and influences that drive the formation and evolution of systems. They also learn to formalize and measure several different aspects of an individual's importance to a system, as well as to formalize and measure various characteristics of the system itself, such as its size, sensitivity to change, and topology (such as its shape and pattern of connectivity). [11]

To earn the network science minor, students take the following five courses to earn the Network Science minor: Fundamentals of Network Science, a theory course, a modeling course, an applications, and a capstone course. Some of the cyber-related skills cultivated in this sequence of courses are how to categorize network types, understand the limitations and challenges associated with network security, build network models to address network security, and identify critical actors in a network. Students will understand the structures associated with various ways network nodes act in the network, formulate processes and structures that degrade, disrupt, and destroy a network, and understand cascading effects of actions in the cyber domain. Students will also learn to understand network sensitivity and understanding cause and effort of network modifications, analyze the influences of human relationships on information, discuss cognitive perceptions and their impact through network interdependencies, and understand the cascading implications of cyber effects on different and common/conflicting mission goals.

WHAT (SOME) CYBER LEADERS SHOULD KNOW: MATHEMATICAL SCIENCES MAJOR

The Mathematical Sciences Major offers abundant opportunities for study in a broad range of mathematical subjects. Courses such as differential equations, linear algebra, mathematical modeling, analysis, numerical computation, statistics, provide a sound mathematical foundation in the science and engineering fields. Also, follow-on courses such as graph theory and networks, linear optimization, combinatorics, and advanced individual study provide both depth in understanding the foundations of mathematical theory, as well as the opportunity for study and research in a selected subject. Whenever possible, cyber is emphasized to extend the knowledge required for the consideration of realistic and challenging problems of today's world. [12]

The Mathematical Sciences department also presents applied mathematical topics and network science needed for success in cybersecurity. We have organized our topics into three areas: modeling large networks, cyber threat discovery, and network dynamics. These topics areas associated with cyber security are challenging and understanding these topics can provide the foundation for many cyber issues. The topics include modeling large networks, discovering cyber threats, and network dynamics.

Modeling Large Networks is covered in the Network Science course (MA394). Here students learn the development of mathematical network models that accurately emulate real-world, multi-layered networks and reflect the dynamics of these real networks. They also use statistical techniques for comparing networks and their properties, and develop methods for efficient computing of network measures. Students learn methods for discovering interesting sub-networks or clusters and optimization and statistical methods for parameter fitting. The course also covers statistical numerical methods for likelihoods of properties.

Discovering Cyber Threats is covered in the Network Science and Optimization courses (MA394, MA481). Students learn about machine learning methods for finding and understanding features for data with evolving characteristics. Students also learn techniques for optimization of properties when using data sampling and data analysis of networks with missing values or attribute uncertainty. They learn how to detect anomalies that do not conform to models to develop understanding the mathematics malicious code detection and understand the aggregation of information (locally and across networks).

The Mathematical Sciences department also presents applied mathematical topics and network science needed for success in cybersecurity.

In the Network Science course, students will also learn network dynamics. They learn how to model flow or the spread of infections or ideas on a network. They also learn game theoretic or dynamical systems techniques for the evolution of cyber threats. Finally, they learn how to employ mathematical models for the emergence of a behavior on networks.

MATHEMATICS SENIOR HONORS THESIS (MA498/MA499)

These two courses provide a year-long thesis option for all math majors. During the year students will produce a research proposal, literature review, midyear report, written thesis, conference presentation, and poster presentation at USMA's projects day. Currently there are four cadets math majors completing year-long honors theses in Cyber related research. Their work includes:

(1) Comparing Statistical Approaches to Anomaly-Based Intrusion Detection Systems, (2) Implementing an Anomaly-Based Intrusion Detection System—Focus on Internal Threat, (3) Finding invariants for the equivalence of quantum error correcting codes, and (4) Investigating the properties of asymmetric key encryption schemes and the effects of transposing the method to different finite groups or elliptical curve space. These yearlong research projects allow cadets to learn a depth of knowledge in a cyber related topic that aligns with their interests.

Past cyber domain related honors thesis topics have also included: (1) The past, present, and the future of wireless security: an analysis of Wi-Fi protected access, (2) Hunting the Zodiak: Attacking the Z340 Cipher with Hybrid Methods, (3) Cryptographic Graphs: A look at the Cryptographic Applications of *Hard* Problems from Graph Theory, (4) Developing an Arithmetic Processor for Elliptical Curve Cryptography and (5) Randomness Properties Found in De Bruijn Sequences.

CYBER EDUCATION BEYOND USMA

The Cyber Branch pilots a program, which affords newly commissioned Cyber officers the opportunity to earn a graduate degree in a cyber-related field before attending their Cyber Basic Officer Leadership Course (CBOLC). It is estimated that ten of the thirty newly commissioned Cyber officers will go immediately to graduate school. Additionally, officers can compete for elite national and international scholarships for additional opportunities to attend graduate school. For example, a current senior cadet was awarded the Churchill Scholarship and will attend Oxford University to earn a one-year Masters of Science degree in Applied Mathematics.

> It is essential that all officers understand how mathematics affect the rapidly developing cyber domain.

The Naval Postgraduate School (NPS) currently offers an applied mathematics education in support of US Army Cyber Command junior officer development. The NPS department of Applied Mathematics has outlined a fully accredited, one year degree program for recent USMA and US Army ROTC graduates that focuses on discrete mathematics and cyber related course work. Students can take optional elective courses in computer science, electrical engineering or operations research. All students will earn graduate certificates in Secure Communications and Network Science. Participants may also be able to earn a third certificate in either Cyber Warfare,Cyber Security Fundamentals or Cyber Security Defense from the Electrical & Computer Engineering or Computer Science departments. [13]

The Air Force Institute of Technology (AFIT) offer graduate programs through its Graduate School of Engineering and Management in engineering, applied science, and management disciplines. It offers masters and doctoral in applied mathematics and operations research: “The aim of the master's degree program is to provide a balanced foundational education in mathematical and statistical analysis, an understanding of appropriate applications of the theory, and some depth in an area of specialization.” [14]

Currently, the Army is offering Advanced Civil Schooling (ACS) opportunities for officers. This fiscal year Advanced Civil Schooling (ACS) is offering fifteen opportunities for Cyber and Electronic Warfare (EW) commissioned officers and warrant officers to broaden their experience and professional career. The target schools are AFIT, Massachusetts Institute of Technology, Texas A&M University, Carnegie Mellon University, NPS, University of California, Berkeley, Georgia Tech, Stanford University, and Virginia Tech. The targeted Graduate Degrees are Computer Science, Applied Math, Information Technology Strategy, Electrical Engineering, Engineering Science, Defense Analysis–Information Operations, and Cyber Operations.

CONCLUSION

There are numerous opportunities for the *Cyber Math* education at USMA, and graduate studies beyond USMA. It is essential that all officers understand how mathematics affect the rapidly developing cyber domain. The USMA Department of Mathematical Sciences is committed to developing an effective mathematics curriculum that attempts to foresee the mathematical needs of tomorrow's students. Emphasis is placed on achieving intellectual discipline, mastery of reasoning, understanding of mathematical concepts, skill in practical applications of mathematics and appreciation for the role of mathematics in the military. The USMA math department produces math majors and network science minors to be strong candidates for Cyber and other technical branches while providing a broad professional cognizance of cyber operations for all students.

NOTES

1. Military Academy CYBER Education Working Group. "Draft Cyber Body of Knowledge." Access on February 10, 2016 form http://computingportal.org/sites/default/files/CEWG%20-%20Draft%20Body%20of%20Knowledge.pdf.

2. Sobiesk, Edward, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor, "Cyber Education: A Multi-Level, Multi-Discipline Approach", SIGITE'15, September 30-October 3, 2015, Chicago, IL, 109-114. Accessed on January 18, 2016 from http://dx.doi.org/10.1145/2656450.2656478.

3. BrainyQuote. "Galileo Galilei Quotes." Accessed January 18, 2016 from http://www.brainyquote.com/quotes/quotes/g/galileogal381323.html.

4. Portia Crowe. The CEO of GE explains why his math degree is more useful than his MBA, Business Insider, 9 December 2015, Accessed January 18, 2016 from http://www.businessinsider.com/jeff-immelt-on-math-and-mba-degrees-2015-12.

5. Military Academy CYBER Education Working Group. "Draft Cyber Body of Knowledge".

6. Sobiesk et. el. Cyber Education: A Multi-Level, Multi-Discipline Approach.

7. USMA Department of Mathematical Sciences, Core Mathematics: Academic Year 2016. Accessed January 21, 2016 from http://www.westpoint.edu/math/SiteAssets/SitePages/Core%20Math/CMB-2015_16.pdf.

8. USMA Department of Mathematical Sciences, Modeling in a Real and Complex World, August 2016, 319.

9. Geisler, Trent. Discussion with author. January 26, 2016.

10. Office of the Dean. "USMA Academic Program (Redbook): Class of 2016." United States Military Academy, West Point, NY. Accessed January 21, 2016 from http://www.usma.edu/curriculum/siteassets/sitepages/course%20catalog/redbook_gy2016_20140509.pdf.

11. USMA Department of Mathematical Sciences, Network Science Minor, Accessed January 21, 2016 from http://www.westpoint.edu/math/SitePages/NetworkScience.aspx.

12. USMA Department of Mathematical Sciences, Mathematical Sciences Major, Accessed January 21, 2016 from http://www.westpoint.edu/math/SitePages/Math.aspx.

13. Naval Postgraduate School, Applied Mathematics Education in Support of US Army Cyber Command Junior Officer Development. Accessed January 26, 2016 from http://www.nps.edu/Academics/Schools/GSEAS/Departments/Math/.

14. Air Force Institute of Technology, Graduate Studies in Applied Mathematics, Department of Mathematics and Statistics Brochure, 2015-2016. Accessed January 21, 2016 from http://www.afit.edu/docs/Brochure2015-16%20with%20cover.pdf.

Bring on the Cyber Attacks – The increased predatory power of the restrained red queen in a nation-state cyber conflict

Dr. Rosemary A. Burk
Dr. Jan Kallberg

ABSTRACT

The militarized and contested Internet with a multitude of state-sponsored cyberattacks can generate an evolutionary process when the targeted nation is strengthened by the abundance of information it receives from the attacks. When the targeted nation restrains from retaliating against the attacking adversarial state its systems are perfected, meanwhile the attacking state is denied the feedback needed to stay current and pose a long-term threat. The targeted nation has increased its potential to go from prey to predator, when the accrued knowledge far exceeds the attacker, and the game has changed. The targeted nation can then strike back far superior on the initial attacker compared to the initial attacker's first moves. In contrast to the Red Queen hypothesis, our Restrained Red Queen model illustrates the adaptive advantage of a targeted nation that decides to selectively counter-strike its aggressor. The reticent targeted nation has benefited from restraining to counter-strike and increases its own survivability by embracing the initial attacks as information that can be converted to superiority over time.

Keywords–cyber evolution; cyber defense; information assurance; cyberwar theory; cyber conflict; cybersecurity

I. INTRODUCTION

This article challenges the common perception that cyberattacks are per default bad and dangerous, and instead argues that cyberattacks carry information vital for the refinement and evolution of the targeted state. Since the dawn of the common Internet, the fear of cyberattacks has been the focal point for the cybersecurity discourse. Cyberattacks carry the seeds for technological development and evolution that drive the ability to go from prey to predator in future cyberwar.

Dr. Rosemary Burk is a Senior Biologist with the U.S. Fish and Wildlife Service, Ecological Services Division in Pacific Northwest Region. Sheearned a Ph.D. in Biology from the University of North Texas with a specialization in aquatic ecology and environmental science. She has co-authored several articles that have linked failed cyber defense and environmental consequences including *Failed Cyberdefense: The Environmental Consequences of Hostile Acts*, which was published by U.S. Army *Military Review* in 2014.

of cyber resilience. The Internet is an ever-evolving online environment with a multitude of actors, but attacks on core nation state functionalities and systems that can degrade the state require substantial resources and intent, which radically limit the number of potential actors to nation states and state-sponsored proxies. The heavy cost and level of dedicated resources to destabilize or shut down a critical system by another state is not in reach for unfunded hackers, terrorists, and cyber criminals.[1] These nation state destabilizing attacks are limited to heavily funded and able actors, which translates to nation states and their agencies.

Cyberattacks that seek to undermine government stability, remove military advantages such as satellite communication, degrade the global information grid and geospatial awareness, impact the financial system, and provide a leverage at a critical juncture in either a low intensity or escalated nation state conflict limits the number of actors. The severity of these attempts and attacks exclude nation states with lower geopolitical postures, and non-state actors. The traditional cyber criminals and the bulk of Internet attacks tend to be vandalism or pursuit of monetary gain, and are in this conflict a background noise of limited importance.

The militarized and contested Internet with a multitude of state-sponsored cyberattacks can generate an evolutionary process when the targeted nation is strengthened by the abundance of information it receives from the attacks. This information is converted through security standards and knowledge consolidation to a higher level of defensive abilities, and the attacks have then strengthened the targeted states. If a nation state instead was denied the cyberattacks that provide information stimulus in adaptive behavior, it will become weakened and over time accumulate numerous unaddressed system vulnerabilities.

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

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

Cyberattacks in their varied forms, appeal to sensationalism due to the tenets of the malicious online activity.[2] Targeted states are perceived not only as risking to lose their citizens' privacy, but also industrial and financial strength, and geopolitical advantages. Furthermore, as every society becomes more reliant upon networked equipment, the reach of cyberattacks has passed a point of being not only a personal threat, but increasingly a national security threat.[3]

Until now, the vast majority of cyberattacks have been of low complexity, lacking precise targeting, and mainly degrade and have non-critical services where the denial of service attacks having been most common.[4] The defense industry, information technology companies, and the defense establishment team up to defend the state against these attacks, and seek to establish a broad militarized ability to hack back on the initial aggressor.[5] The growing number of attacks are frustrating, and as of today it is illegal for any private entity to hack back in the US[6] and the UK,[7] but there is a strengthened political acceptance for allowing a wider use of hacking back,[8] maybe even beyond the governmental agencies' realm. The US Congress endorsed the "Commission on the Theft of American Intellectual Property", which proposed a model for corporate hack back to enable corporations to strike back if attacked,[9] addressing the lack of governmental response to the increasing number of cyberattacks by allowing corporations to take action by themselves. Even if there have been concerns voiced from the business community,[10] the paradigm, in both commercial and government cyber security, is that hacking back is an opportunity.

II. THE RESTRAINED RED QUEEN

The first question, from a strategic standpoint, is hacking back warranted? As long as the cyberattacks are unsystematic, and of moderate complexity, these attacks pose marginal risk for the targeted nation. An alternative approach is that the targeted nation decides not to, on a routine basis, hack back, and instead utilizes the information delivered by initial attacker to the targeted nation's advantage. This article challenges the common perception that cyberattacks are per default unacceptable and dangerous, and introduces the concept of the restrained Red Queen. [11] [12]

In nature, there is a never-ending evolutionary arms race between predator and prey: the Red Queen Hypothesis. [13] [14] This model, the Restrained Red Queen, represents the targeted nation that refuses to play the evolutionary *tit-for-tat* game, [15] but instead silently and passively collects information from the cyberattacks, and in doing so changes from prey to predator. The claim in this article is that unilaterally not striking back can strategically create decisive capability instead of engaging in a never ending *tit-for-tat* set of digital interchanges with the attacker with no decisive end in sight.

Cyberattacks carry the seeds for technological development and evolution that drive the ability to go from prey to predator in future cyberwar.

The Internet has become a contested and militarized public space, where weak attribution and absence of global norms enables aggressive and adversarial nations to launch numerous cyberattacks on other countries, and their institutions. Nation states rush to create military cyber units for their defense, and views the open Internet as a national security threat [16] that has to be regulated, contained, and managed. [17] [18] The attacker is considered to be in a stronger position, based on the two unique tenets of the Internet: limited attribution and accountability. [19]

Nations address cyber defense in traditional military terms of attack, defense, and territorial defense lines. Military theory evaporates in cyber, because it does not take into account the unique cyber challenges: anonymity, lack of object permanence, and absence of measurement of effectiveness. Conventional military thinking is burdened by tradition and assumptions of its applicability in past solutions, which makes traditional military theory spurious in cyber. Instead, if the thoughts are aligned with the unique tenets of cyber, then ignoring the attacks is a viable option.

III. CYBER EVOLUTION AND ENTERPRISE PATCH MANAGEMENT

The present-day preparation for a future cyberwar assumes that the developments are a classic evolution with innovation, adaptation, and interchanges of predatory behavior where both sides in a cyber-conflict are engaged and drive each other's evolution, where at the end you have one winner. The predatory states and the targeted states are assumed to co-evolve to a higher level of cybersecurity development. This assumption has a critical flaw—the restrained cyber Red Queen that does not strike back is better positioned than the counter striking Red Queen.

The Western and industrialized world uses information security management systems that are designed according to the Plan-Do-Check-Act methodology (PDCA).[20] The PDCA-cycle originates from traditional industry quality assurance in the 1950s, and is also referred to as the Deming's cycle.[21] [22] The information security management systems (ISMS) are the overarching methodology to protect larger information systems. [23] [24] The ISMS is created to self-adjust and remove vulnerabilities over time.[25] [26]

The density of vulnerabilities[27] matters because the greater the number of vulnerabilities in a targeted system, each patch is less effective as a countermeasure. If an attacker by the attack has exposed a vulnerability in a system with 100 vulnerabilities, the following patch and removal of the vulnerability would then have taken care of 1% of the vulnerabilities. A larger well-maintained system, such as a nation state pivotal information system, will have fewer critical and potentially system destabilizing vulnerabilities than consumer software and smartphone apps.[28] As an example, the US government increases spending on cybersecurity and the federal cybersecurity project is a multi-billion dollar enterprise.[29] In contrast, 50% of all enterprise smartphone apps have been developed without a budget to address security.[30]

> The reach of cyberattacks has passed a point of being not only a personal threat, but increasingly a national security threat.

National systems have fewer and less dense vulnerabilities, which allows the national IT systems to heal faster and consolidate the understanding of the vulnerabilities within the organization in a timely manner.

The more attacks that are launched on the national information systems, especially attacks that are unsystematic and of lower and moderate technical complexity, the stronger the defenses become in the targeted nation. A breach of information security, a system penetration through the firewalls and internal defensive measures, leads to an incident report and the systems then use the information to create a solution to avoid a future breach. In the industrialized world, these software and hardware solutions are custom-made for industries and government, where the residual vulnerabilities are fewer and less dense due to high cost-acceptance for maintenance, systematic approach, active penetration testing, and system overhauls.

The vulnerabilities that affect the general public and their home computers, such as viruses, malicious malware, and adware receive patches for their client machines by Internet security vendors and software vendors.

Corporations and government agencies are rapidly and uniformly working to deploy patches and software code updates to remove vulnerabilities,[31] and by doing so ensure healing of their IT-systems from similar future attacks by an adversarial state. Prolonged series of attacks would trigger incidents leading to rigorous securing of pre-existing vulnerabilities in the key information systems in the targeted society.

If the number of residual vulnerabilities were 100 to start with, every exposed vulnerability reduces the total exposure to these vulnerabilities by 1%, and over time the reduction of these vulnerabilities reach levels where there are less vulnerabilities available for an attacker in a future cyber conflict to destabilize and impact policy in the targeted society. By absorbing these attacks as information, healing one by one the sparse number of vulnerabilities, the targeted nation state government reaches a higher level of cyber resilience, and ability to operate in a degraded environment.

This article challenges the common perception that cyberattacks are per default unacceptable and dangerous, and introduces the concept of the restrained Red Queen.

Over time, the targeted nation will gain an evolutionary advantage over the aggressive nation by unilaterally restraining from counterattacks, and instead use the feedback loop generated by the attacks to its advantage by healing the systems, and at a later stage strike back decisively. A cyberattack that penetrates the firewall and defenses of the targeted system is a set of information that generates in standardized information security management system (ISMS) an incident report that leads to the creation of a solution to the vulnerability. The solution to the vulnerability is a set of customized programming that is distributed and implemented through the organization. These software updates are called patches. If the vulnerability is related to a specific software, the software vendor will use the incident information to create their commercial security update, patch, and then distribute it to their customers.[32] Therefore, in theory, one single identified attack can lead to the updating of millions of client computers and a rapid sharing and dissemination of risk information followed by mitigation on a broad scale.[33]

IV. FEEDBACK DENIAL AND REVERSAL OF PREDATORY POWER

If a targeted nation restrains from counter striking their attacker with cyberattacks, then the initial attacker is denied the feedback loop that would benefit their systems. As long as the Restrained Red Queen does not strike back, the advantage can increase.

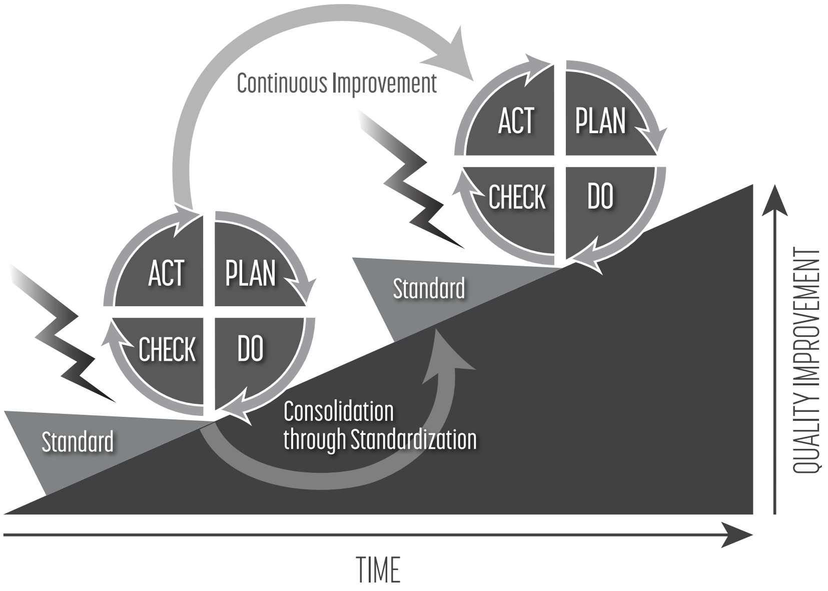


Figure 1. The cyberattacks strike the system and trigger incidents in the *Check* area in the PDCA cycle leading to continuous improvement and consolidation through standardization, which drives the targeted nation's development. Image source: Wiki Commons (modified).

Darwinism in cyberspace works elegantly—the system that is able to adapt and respond to information in the feedback loop survives. The Restrained Red Queen that refuses to strike back then will by her unilateral actions be superior at a later point in time when she decides to strike back. The Restrained Red Queen has perfected her systems and patched her vulnerabilities.

Over time, the attacking society accumulates numerous unexploited vulnerabilities that increase when new systems are added, the width of technology usage increases, and older legacy systems still exist in a mixed environment. Under attack, the restrained Red Queen facilitates software patches and vulnerability mitigation left undone by the initial attacker.

Then the Red Queen turns around utilizing automated collection of vulnerabilities against the initial attacker. A systematic automated collection of vulnerabilities can be used to scan the adversarial systems for vulnerabilities, store the vulnerabilities in an attack repository, and then launch a disproportional digital response by a massive counterstrike. The restrained Red Queen has then turned the table and prey becomes predator.

The rabbit runs faster than the fox, the rabbit survives by being faster. In cyber, any nation can be a fox if it chooses to do so, and the power of rapid digital execution increases the number of predators available in the future. In the cyber revenge of the Restrained Red Queen, the fox chases the rabbit. The rabbit becomes more of a predator the longer the fox runs and the fox is weakened. At a point in time the rabbit turns around and

Nation states operate in an environment where the systems are larger with complex structures and sparse vulnerabilities as a result of active maintenance and the pursuit strikes back with lethal power. The multitude of cyberattacks on the targeted society has trained the society, created cyber resilience, leveraged the knowledge about exploits, honed and tuned future vulnerability harvesting systems, and through these feedback loops the healed the vulnerabilities. The prey has gained a superior technical advantage and may exploit the weaknesses of the aggressor.

V. ADVERSARIES ON THE BRINK TO ENTROPY

The cyberattacks' utility is determined by the societal institutional design of the targeted nation. A targeted state that has solid and stable institutions is more resilient than a state with weak institutions and lingering entropy.[34] The current cyber engagements between nation states do not occur between states of equal or similar institutional design. China, Iran, and Russia are states where the existence of the current regime is dependent on suppression of opposition and in some cases, suppression of the popular will. The countries that are actively cyber adversarial to the United States, United Kingdom, Sweden, France, Australia, Japan, and Germany are weaker states with fragile institutions.[35] A cyber conflict is fought through the whole society,[36] within digital reach, and weak institutions and a suppressed popular will can destabilize a totalitarian regime. It is unlikely that cyber units in any of the nation states, by the cyber units' sheer size and abilities in relation to the infrastructure and size of the national economy, will have a measurable influence on the developments of a future cyber conflict. Instead, cyber defense relies primarily on already existent cybersecurity measures in the public and private sector. The main contribution the state offers is coordination and direction. Even if North Korea and Iran have designated cyber units, the units' actual influence in the event of a major counter strike is marginal, if any. The key weaknesses in the adversarial nation's cyber defenses are the lack of decentralization, initiative, and structured ways to create patches and distribute these patches due to the totalitarian institutional design of these states.

> The cyber evolution is a process where pressure from an external environment leads to natural selection and adaptation.

Therefore, the risk for a regime to become destabilized due to cyberattacks is higher in China, Iran, and Russia than in the United Kingdom or Switzerland, which are countries with very high institutional stability. For the restrained Red Queen this is important, because a counter strike does not need to be perfect to jeopardize the stability of the initial attacker. The lingering dormant entropy embedded in the weak institutional framework of the initial attacker can become a force multiplier in the counter strike.

VI. EVOLUTIONARY DENIAL

The cyber evolution is a process where pressure from an external environment leads to natural selection and adaptation. The adaptation occurs as a response to unilateral attacks. By not immediately counter striking, the targeted nation deprives the initial attacker of information that would support its ability to adapt and address its vulnerabilities. Those societal systems that are best adapted to their environment will survive, and societies that do not adapt and correct its vulnerabilities perish.[38] The adversarial predators becomes over time prey in digital Darwinism.

VII. CONCLUSIONS

The general assumptions that cyberattacks are all malicious events does acknowledge the evolutionary potential generated from cyberattacks as each attack is a set of delivered information to the target. Therefore, continuous and unsystematic attacks are important for any defender in cyber war as it first triggers the feedback loop in the PDCA driven ISMS, leading to an improvement in internal defensive measures and on a larger scale drives consolidation through standards and information sharing. The information sharing is either through direct collaboration between entities with in the same industrial group or through information system vendor based patch management that distributes the additional software needed to protect the system. On a national scale dispersed attacks over a series of targeted companies and public entities creates a national resolution to that specific software vulnerability. The attacks have then generated a leveraged cyber defense posture for the targeted state.

> If a targeted nation restrains from counter striking their attacker with cyberattacks, then the initial attacker is denied the feedback loop that would benefit their systems.

If the targeted nation refuse to engage in a *tit-for-tat* cyber conflict, but instead unilaterally holds back, the attacking state is denied the information that would trigger their cybernetic healing by the activation of their feedback loop and consolidation through standards and patch management.

Although cyberattacks within the past decade have been regarded in mass media as a monumental national security threat, they have instead generated the targeted countries' cyber-resilience by delivering vulnerability information and trigger extensive healing of the national information systems, leading to improvements instead of havoc.

The views expressed herein are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, the Department of the Interior, the Department of Defense or the Department of the Interior.

NOTES

[1] J. Michaels, (2013, April 21), "Pentagon expands cyber-attack capabilities," *USA Today,* Available at: http://www.usatoday.com/story/ news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/.

[2] E. Bumiller and T. Shanker, (2012, Oct. 11), "Panetta Warns of Dire Threat of Cyberattack on US," *New York Times.*

[3] W.J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* September 2010, 97-108.

[4] W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congressional Research Service,* Library of Congress, 2004, 7.

[5] J. Kallberg, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," *IEEE IT Professional,* pp. Jan.-Feb. 2015, 30-35.

[6] 18 U.S. Code § 1030, 'Fraud and Related Activity in Connection with Computers', *United States Code,* title 18, part I, chapter 47, 1986.

[7] H.M. Government, Computer Misuse Act 1990, Parliament of the United Kingdom.

[8] C.M. Matthews, (2013, June 2), "Support Grows to Let Cybertheft Victims 'Hack Back," *Wall Street Journal Online.*

[9] Commission on the Theft of American Intellectual Property, the *IP Commission Report,* 22 May 2013.

[10] J. Westby, (2012, Nov. 12), "Caution: Active Response to Cyber Attacks Has High Risk," *Forbes,* Available: <www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk>.

[11] L. Van Valen, "A New Evolutionary Law", *Evolutionary Theory* vol. 1, 1973, 1-30.

[12] G. Bell, *The Masterpiece of Nature: The Evolution and Genetics of Sexuality,* Berkley, USA: University of California Press, 1982.

[13] L. Van Valen, "Molecular Evolution as Predicted by Natural Selection," *Journal of Molecular Evolution* vol. 3/2, 1974, 89-101.

[14] L. Van Valen, "The Red Queen," *American Naturalist,* 1977, 809-810.

[15] . B. Quental, and C. R. Marshall, "How the Red Queen Drives Terrestrial Mammals to Extinction," *Science* vol. 341/6143, 2013, 290-292.

[16] J. A. Lewis, "National Perceptions of Cyber Threats," *Strategic Analysis* vol. 38/4, 2014, 566-576.

[17] K. B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* vol. 46/3, 2007.

[18] J. Kallberg, and B. Thuraisingham, "Cyber Operations Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly,* vol. 68/1, 2013.

[19] D. T. Fahrenkrug, "Countering the Offensive Advantage in Cyber-Space: An Integrated Defensive Strategy" in proceedings of the 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn , 2012, 197-207.

[20] C. Pelnekar, "Planning for and Implementing ISO 27001," *ISACA Journal,* vol. 4, 2011.

[21] N. R. Senapati, "Six Sigma: Myths and Realities," *International Journal of Quality & Reliability Management,* vol. 21/6, 2004, 683-690.

[22] Y. Kondo, "Emphases of Japanese Total Quality Management in the 1980s," *Total Quality Management* vol. 1/1, 1990, 23-32.

[23] D. W. Straub, and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly,* 1998, 441-469.

[24] F. O. Sveen, J. M. Sarriegi, E. Rich, and J. J. Gonzalez, "Toward Viable Information Security Reporting Systems," *Information Management & Computer Security,* vol. 15, 2007, 408-419.

[25] C. N. Johnson, "The benefits of PDCA," *Quality Progress,* vol. 35/5, 002 120.

[26] R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799," *Information Management Journal* vol. 39/4, 2005, 60-66.

[27] Bruce Schneider, (2014, May 19), "Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?," *The Atlantic,* Available: http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/.

[28] S. R. Femerling, Vulnex, Available: http://media.blackhat.com/bh-eu-12/Rose/bh-eu-12-Rose-Smartphone_Apps-WP.pdf.

NOTES

29. A. Shalal and A. Slyukh, (2015, Feb. 2), "Obama seeks $14 billion to boost U.S. cybersecurity defenses," *Reuters Online,* Available: http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202.

30. L. Ponemon, IBM, "IBM-Sponsored Ponemon Institute Study Reveals Alarming State of Mobile Security for Apps," Available: http://securityintelligence.com/mobile-insecurity/.

31. T. Gerace, and H. Cavusoglu, "The Critical Elements of the Patch Management Process," *Communications of the ACM,* vol. 52/8, 2009, 117-121.

32. H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security Patch Management: Share the Burden or Share the Damage?," *Management Science,* vol. 54/4, 008, 657-670.

33. B. Brykczynski, and R. A. Small, "Reducing Internet-based Intrusions: Effective Security Patch Management," *IEEE Software,* vol. 20/1, 2003, 50-57.

34. J. Kallberg, B. Thuraisingham, and E. Lakomaa, "Societal Cyberwar Theory Applied: The Disruptive Power of State Actor Aggression for Public Sector Information Security", in proceedings of the IEEE EISIC European Intelligence and Security Informatics Conference, 2013, 212-215.

35. L. Chaudhary, A. Musacchio, S. Nafziger, and S. Yan, "Big BRICs, Weak Foundations: The Beginning of Public Elementary Education in Brazil, Russia, India, and China," *Explorations in Economic History* vol. 49/2, 221-240, 2012.

36. J. Kallberg, and R. A. Burk, "Cyber Defense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations' in Conflict and Cooperation in Cyberspace – The Challenge to National Security in Cyberspace, Panayotis A. Yannakogeorgos and Adam B. Lowther, Eds., New York, NY: Taylor & Francis, 2013.

37. J. Kallberg, and R. A. Burk, "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," *Military Review,* vol. 3, 2014, 22-25.

38. S. J. Gould, "Ever Since Darwin: Reflections in Natural History," New York, NY: WW Norton & Company, 1992.

U.S. Special Operations Forces in Cyberspace

Colonel Patrick M. Duggan

with special contributions from
Elizabeth Oren

C*yberspace is a human space, as dynamic and uncertain as human nature.* No longer simply a technical abstraction or manmade domain unto itself,[1] cyberspace is a growing facet of every-day life that increasingly cuts across all aspects of Special Operations. Cyber is a dynamic space, a global commons of human practice, which embodies the actions, behaviors, and decisions of man. Cyber is also an uncertain space; and although, its future impact to our national security is yet to be determined, it is clearly a space where United States Special Operations Forces (USSOF) have an increasing role in shaping the final outcome. Ultimately, cyber is a human enterprise which empowers and entangles countless global interactions,[2] and is rapidly becoming a preeminent space where human conflicts, and thus USSOF, must play a part.

Cyberspace

The enigma of cyberspace is in its contradictions. Cyber is both everywhere and nowhere at the same time, casting an invisible, yet powerful influence, which brings both comfort and stress to every-day life. On one hand, cyberspace helps foster human prosperity by flattening opportunities and improving quality of life. On the other hand, cyberspace inflames ethnic and religious tensions, sows dissent, and causes suffering. It is in these contradictions where cyberspace is most like human nature, and it is in these same spaces, both challenges and opportunities exist for USSOF.

Cloaking their roles and obscuring their actions, adversaries are increasingly exploiting the shadows of cyberspace to attack US national security interests. Ranging from lone cyber-terrorists, to state-sponsored cyber-units, adversaries use cyberspace's low barriers of entry, difficult attribution, and lack of clear borders for battle[3] to conceal their reckless ambitions. Fortunately, while adversaries may exploit cyber to strike from the shadows, it is in these same shadows USSOF must pursue, to help illuminate, uncover, and counter the growing array of technologically-savvy threats plaguing our nation.

Colonel Patrick Duggan is the Commander of Joint Base Myer-Henderson Hall in Washington D.C. He is a career Special Forces Officer, and participated in both invasions of Afghanistan and Iraq, and commanded Special Operations deployments across the Middle East and Asia. A Certified Information Systems Professional (CISSP), COL Duggan has authored numerous articles about Cyber-Special Operations in Joint Defense Quarterly, Special Warfare Magazine, Small Wars Journal, and The Cyber Defense Review, and is the recipient of the 2015 Chairman of the Joint Chiefs of Staff Strategic Research and National Security Award for his paper, *Strategic Development of Special Warfare in Cyberspace*. COL Duggan is a 2+/2+ Arabic speaker with varying proficiency in Tagalog, French, and Spanish.

National Cyber Roles

The Commander of the United States Cyber Command and Director of the National Security Agency, Admiral Mike Rogers, recently wrote that "No single entity has all the necessary insight, authorities, capabilities, or resources to protect and defend US and allied interests in cyberspace," [4] and I couldn't agree with him more. Cyberspace is not just an intelligence or communications thing; it is an 'everybody thing.' This includes the way in which we marshal the talent and intellect of our military, interagency, and private sector leaders, to build whole-of-nation strategies to protect the US.

The ubiquity of cyberspace means that no single US Agency, Department, or Service Component owns the market on good ideas, so it is imperative that we harness our country's diverse experience, amongst all institutions, to promote ever-adaptive strategies which secure our nation. We must also seek and examine new concepts, processes, and approaches to deal with these dynamic challenges, and each does our individual part, in a collective contribution to our national defense.

Special Operations Forces (SOF's) National Contribution

Part of SOF's contribution to confronting our nation's cyberspace problems, is asking ourselves how to best harness our own strategic strengths, and do it in a manner which best navigates cyber's dynamic and uncertain human nature. SOF's strategic value for the nation is in its unique small footprint, exercised through a global network of partners, providing persistent engagement and partner enablement, as well as, discreet and rapid response. These same strategic strengths provide new unconventional opportunities and asymmetric options that must be further developed and integrated into our national cyber-strategies.

Whether conducting virtual Foreign Internal Defense (FID) to build partner security and capacity, or executing cyber-enabled Direct Action (DA) to eliminate hostile threats, cyberspace amplifies "the elemental aspects of what makes a special operation, special." [5] Meaning, cyberspace amplifies a DA mission's lethality, precision, and discreet nature; while in FID's case, cyberspace amplifies connectivity, capability, and trust. [6] It is increasingly clear that every USSOF mission must be amplified by cyber so that we can evolve our strengths into new strategic instruments to protect and project our national interests.

SOF is Dynamic

With every passing day, our hyper-connected landscape seems to produce a new class of threats, more technologically evolved than the last, harnessing the explosion of technology, information proliferation, and network connectivity for ambiguous warfare. [7] This means that, "in the not too distant future, every Special Operations Forces practitioner will be required to understand the basics of cyberspace, computers, and coding; not because they're expected to be programmers, but because they'll need those skills to conduct special operations in an era vastly more interconnected than now." [8] USSOF must rapidly adapt and evolve, as they increasingly find themselves pitted against tech-savvy adversaries in dynamic situations, where they must employ some of the same cyber-technologies in unconventional ways. From high-tech to low-tech, and from human-centric to techno-centric, USSOF will employ cyber-technologies as a means to directly or indirectly strengthen our global network of partners, and amplify our unique capabilities exercised through a wide-array of options.

> Cyber is both everywhere and nowhere at the same time, casting an invisible, yet powerful influence.

USSOF will employ cyberspace as a means to better understand the passions, which drive human action and behavior, and will use cyberspace as a vehicle to identify conflicts earlier, seize opportunities to steer, and potentially, tamp down violence. [9] Synthesizing objective technical data with subjective human understanding, USSOF will develop a deeper nuanced understanding of global and regional situations. USSOF will also generate new thinking and unconventional approaches to recruit people to noble causes, and use cyberspace as a means to engender the positive aspects of human behavior, such as decentralized and participatory action. Using their access, placement, and most importantly their influence, USSOF will help build holistic networks, which support national cyber-strategies, and assist in weighing psychological and technical acts against the competing needs for secrecy and credible action.

Just like cyberspace, USSOF operations are not a monolithic enterprise dependent upon one tightly woven centralized system. Instead, USSOF operations resemble cyberspace itself, resiliently designed to leverage global networks riding across open architectures. Meaning, USSOF can assemble, swarm, disaggregate, or even replace one another, without disrupting the rest of the system. As with cyberspace, USSOF networks are a heterogeneous mix of Joint, Coalition, and other partners whose operations can be scaled up or down to attack and defend human and information networks. Similar to cyberspace, USSOF operations are not dependent on just a handful of brittle nodes, but operate across vibrant, expansive, and living global networks. Most importantly, just like cyberspace, the true power of USSOF operations are the humans behind them.

SOF Thrives in Uncertainty

In a recent speech, Director of National Intelligence (DNI), James Clapper, stated that cyber threats to US national security are increasing in frequency, scale, sophistication, and severity, and that since 2013, have "bumped terrorism out of the top spot on our list of national threats." [10] Adding that the trend will continue, the DNI underscored the importance of having "the best minds of our nation working this range of cyber problems." [11] Making matters particularly acute for USSOF, is that global terrorism and weapons of mass destruction (WMD) and proliferation perennially top the list of national security threats. This dangerous mix of cyberspace threats, terrorism, and WMD is a volatile brew, and poses serious dangers to the nation, in which USSOF must not fail.

> With every passing day, our hyper-connected landscape seems to produce a new class of threats, each more technologically evolved than the previous.

Although these are serious challenges, it is in adversity where USSOF best excel. USSOF is specially trained for ambiguous conflict, and thrive in complex challenges, which do not always lend themselves to obvious approaches. [12] With no clear decisive points or geometries in battle to guide them, USSOF must blaze new trails in an ever expanding wilderness of dangerous and complex problems. Our national defense requires unconventional approaches to counter unconventional problems, so USSOF will not only employ new cyber-technologies, but more importantly, innovate new concepts and tactics to do it. USSOF will fuse emerging capabilities into time-tested practice to create new solutions and provide new strategic opportunities for the nation.

As an example, envisioning options for future command and control relationships, such as the creation of a Special Operations Command-Cyberspace (SOC-CYBER), as a means to provide national strategic capabilities and specialized expertise no other DoD service can provide. [13] A SOC-CYBER could enrich perspectives during the development of national cyber-strategies, and infuse unconventional insights and asymmetric options during the process.[14] USSOF could also relay observations from the field, derived from their global footprint, to add nuance and context to some of the human-complexities of psychological, cultural, and societal dynamics; then, discreetly tie back into ongoing operations.[15] Ultimately, investing USSOF in cyber-organizations mixes some of the best and brightest US talent and expertise, and the diversity of its spirit is in the best interest of our nation.

Keys to a Human Space

USSOF operations provide keys to unlocking deeper understanding of human interactions in cyberspace, and a means to contextualize the sociocultural, political, and historical factors which all too frequently fuel strife.[16] Cyberspace provides USSOF new opportunities to leverage culture to build relationships, and deter our adversaries with a wide array of lethal and non-lethal options. Cultural intelligence equates to influential power,[17] and its instrumentality is driven by humans in cyberspace.

Successfully navigating our hyper-connected world means better understanding its cultural landscape, and requires blending emerging cyber-technology with unconventional approaches. Using cultural intelligence as an emerging tool, USSOF can better target, influence, degrade and destroy our nation's shadowy adversaries.[18] Whether they operate virtually via social media, or through digital communications, an adversary's human networks remain physical, and are susceptible to cross-cultural and transnational targeting. Despite attempts to conceal their actions, USSOF can find points of leverage in the cultural details to influence strategic outcomes with cyber capabilities.[19]

The US must continue to work together to confront vast cyber challenges by increasing our collective institutional efforts.

Providing persistent partner engagement is increasingly dynamic, as the convergence of cyberspace and the physical world cause both partners and adversaries to assume different roles depending on the circumstance. It is increasingly important to correctly interpret events, information, and disinformation, so that USSOF can more accurately influence outcomes in any environment, in any situation, no matter the actor.[20] This will require USSOF's unique access and placement, and most of all, their influence, to better understand the increasingly complex cultural cross-sections of human and digital interaction.

Although it is clearly an uncertain world, USSOF will use their cultural expertise in building cyber-partnerships to better assess partner realities, strengths, and vulnerabilities,[21] and ensure USSOF provide culturally attuned security assistance. Additionally, USSOF will evaluate the social and economic factors shaping partner circumstance, to ensure they provide culturally compatible means and solutions for partners to solve their own problems, once USSOF depart. USSOF will also use cyberspace to understand better their partners' cultural values, and examine where and how our nation's values square against the enduring viability of potential relations, [22] and better calibrate US support accordingly.

Cyberspace is rapidly changing the world's cultural landscape and will increasingly challenge and redefine traditional concepts of society and national identity. [23] The proliferation of cyber-technology pressures cultures to change, and requires USSOF to keenly monitor cultural trends, as cultural dynamics steadily shape world events and competing perspectives. Cultural intelligence is a part of USSOF's approach to understand better evolving cultural dynamics, and cyber is the indispensable space to harnessing new strategic opportunities for the nation.

Conclusion

The contradictory nature of cyberspace will continue to shape our lives, as it does our national security. Just like the human's cyberspace emulates, cyber is dynamic and uncertain, and presents both serious challenges and unrealized opportunities for USSOF and our nation. The US must continue to work together to confront our vast cyber challenges by increasing our collective institutional efforts, as well as, challenging our respective organizations on ways to improve what we individually bring to the table. Although cyberspace's future impact on national security is yet to be determined, it is increasingly clear that USSOF will have an expanding role in shaping the outcome. Ultimately, cyberspace is a human space; and, it is exactly where USSOF needs to be.

Special Contributor

Elizabeth Oren

Elizabeth Oren specializes in cultural analysis, and supports both conventional and SOF communities with qualitative analytics. Over the last 10 years, Ms. Oren has conducted specialized research on refugee and immigration trends, machine translation, and cultural networks. Ms. Oren has worked in France, Turkey and Germany, and is a graduate of Texas A&M University and the University of Texas at Arlington holding degrees in international studies and foreign languages.

NOTES

1. Patrick Duggan, "Harnessing Cyber-technology's Human Potential," *Special Warfare 28,* no.4 (October-December 2015), 12. http://www.soc.mil/swcs/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf (accessed February 25,2016).

2. Patrick Duggan, "Why Special Operations Forces in US Cyber-Warfare?" *Cyber Defense Review,* January 8, 2016, 1. http://www.cyberdefensereview.org/2016/01/08/why-special-operations-forces-in-us-cyber-warfare/(accessed February 22, 2016).

3. Ibid., 3.

4. Michael S. Rogers, "A Challenge for the Military Cyber Workforce," *Military Cyber Affairs:* Vol. 1: Iss. 1, Article 2. (2015), 1. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1012&context=mca (accessed March 2, 2016).

5. Patrick Duggan, "Man, Computer, and Special Warfare," *Smallwarsjournal.com,* January 4, 2016, 4. http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare (accessed February 22, 2016).

6. Ibid., 4.

7. "Man, Computer, and Special Warfare," 1.

8. Patrick Duggan, "SOF's Cyber FRINGE," *Smallwarsjournal.com,* February 10, 2016, 1. http://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe (accessed February 22, 2016).

9. "Why SOF in US Cyberwarfare?" 8.

10. Aaron Boyd, "DNI Clapper: Cyber Bigger Threat than Terrorism," *FederalTimes.com,* February 4, 2016, 1. http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/ (accessed March 2, 2016).

11. Brian Murphy, "Director of National Intelligence Visits USNA for Cyber Lecture," *The Trident,* February 18, 2016, 1. http://usnatrident.blogspot.com/2016/02/director-of-national-intelligence.html (accessed March 2, 2016).

12. "Why Special Operations Forces in US Cyber-Warfare?" 7.

13. Ibid., 8.

14. Ibid., 8.

15. Ibid., 8.

16. Patrick Duggan, "Strategic Development of Special Warfare in Cyperspace," *Joint Forces Quarterly 79,* (4th Quarter 2015): 49. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/621123/jfq-79-strategic-development-of-special-warfare-in-cyberspace.aspx (accessed February 22, 2016).

17. Elizabeth Oren, "Culture in a Murky World: Molding the Field of Cultural for International Security," *University of Texas at Arlington, Iss.1* (unpublished) 4.

18. Elizabeth Oren, *"Report on Islamic State's Asymmetric Information Campaign,"* (Oberammergau, Germany: NATO, January 4, 2015) 4.

19. "Culture in A Murky World", 5.

20. Elizabeth Oren, "A Dilemma of Principles", *Special Operations Journal,* Spring 2016, 8. Vol. 2, No. 1.

21. "Culture in a Murky World", 6.

22. Ibid., 6.

23. Ibid., 6.

Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex

Dr. Mark Raymond

Security and intelligence practitioners are rapidly expanding their cyber capabilities to accomplish their core missions of warfighting, ensuring homeland security and advancing national security interests. However, their efforts also have significant implications for a large and expanding array of other actors, rules and institutions at both the domestic and global levels. This article discusses the emerging global regime complex for cyber issues, highlighting contemporary rule-making challenges and the potential for international conflict over the nature of the cyber regime complex. It then demonstrates the importance and the difficulty of engaging security and intelligence practitioners more closely with these processes of global rule-making, and argues that such efforts must begin at the cultural and attitudinal levels within the broader intelligence and defense communities. The article concludes by advancing modest recommendations for next steps in ensuring the engagement of security and intelligence practitioners with the global cyber regime complex. It recommends: (1) the augmentation and expansion of secondment, fellowship and exchange programs, to ensure as much dialogue and mutual learning as possible; (2) the institutionalization of capabilities for states to engage in good-faith troubleshooting when the activities of their security and intelligence practitioners have unintended negative effects on others; (3) the institutionalization of responsibility to actively consider the effects of policies, programs, and operations both on specific third parties and on the global public interest; and (4) the active promotion of all of the foregoing measures in all states that begin to develop significant cyber capabilities.

The Emerging Cyber Regime Complex

Contrary to media assertions that the Internet is an ungoverned Wild West, the Internet could not exist without a complex and robust array of rules. Internet protocols (TCP/IP, BGP, SSL, html, etc.) and hardware standards are only the tip of the iceberg.

Many such examples have escaped notice as a result of high levels of private and non-profit governance that have caused citizens and policymakers to take the Internet's continued existence for granted rather than treat it as the ongoing social accomplishment it truly is. Because the Internet is an ongoing social accomplishment in addition to a collection of physical infrastructure, governance issues are central to the ways in which cyber-conflict is evolving and will continue to evolve. Changes in these governance mechanisms will shape what is possible, what is likely, what is easy or difficult, and what is expensive or inexpensive. Further, there are increasing indications that a key subset of cyber conflict will revolve precisely around contesting the nature and form of these governance mechanisms. That is, cyber conflict is not merely about offensive and defensive cyber operations by state and non-state actors. It also includes attempts to shape how the administration and use of the Internet is governed. This latter dimension of (potential) cyber conflict is fundamentally a problem of rule-making. While much of this rule-making happens at the global level, the interconnected nature of the Internet at the physical and logical layers means that domestic policy and the actions of domestic firms and non-state actors can have significant negative externalities.[1] Accordingly, there are critical pressures for global coordination and cooperation on many dimensions of Internet governance even beyond the technical requirements for globally unique Internet Protocol (IP) addresses and Internet domain names (DNS).

Scholars of International Relations (IR) have understood these attempts to create policy coordination above the level of the state through the concept of an international regime. A regime in this sense is a

Mark Raymond (@mraymondonir) is the Wick Cary Assistant Professor of International Security at the University of Oklahoma and a Fellow with the Center for Democracy and Technology. His work appears in International Theory, the Georgetown Journal of International Affairs and the Canadian Foreign Policy Journal. He is also the co-editor of Organized Chaos: Reimagining the Internet (Waterloo, Canada: CIGI, 2014). He has testified before the United Nations Commission on Science and Technology for Development, and participated in the Internet Governance Forum. His current research projects examine the politics of global rule-making, as well as Internet governance. He received his Ph.D. from the University of Toronto.

set of implicit and explicit principles, norms, rules and decision-making procedures that set rules of the game and shapes expectations among actors. Regimes have typically been delineated by substantive issue-areas.[2] While interconnections between different issue-specific regimes have been noted, both practitioners and scholars have (until recently) usually treated them as analytically separate entities. As a result of globalization and the increasing density of global governance mechanisms, this analytic choice may be unsustainable. For instance, Joseph S. Nye, Jr. has argued that the narrow Internet governance regime is more usefully seen as embedded in a broader cyber regime complex.[3]

A regime complex refers to a connected set of regimes that have common subject matter, at least partially overlapping membership and (as a result) generate problematic interactions.[4] For example, attempts to deal with intellectual property rights enforcement are proceeding simultaneously through the international trade regime as well as through the Internet governance regime and through domestic courts and legislatures. Similarly, attempts to create rules of the road for state conduct online are evident in the United Nations, through the Group of Governmental Experts (GGE), as well as in particular bilateral relationships (e.g. the US and China) and in NATO. There is no guarantee that the outcomes of these distinct processes will be complementary or even compatible. As a result, there is a greater need than in the past to 'deconflict' formerly distinct regimes that are now creating or that could create negative externalities for each other. Because many of these rule-sets will pertain to the work of security and intelligence practitioners, it is vital that these communities be involved in such deconflicting efforts.

While Nye is right to suggest the need to focus on the broader cyber regime complex in addition to the narrower Internet governance regime, it is important to recognize that the cyber regime complex is still in the early stages of formation. These processes of figuring out how to manage new (or at least newly salient) interactions between established rules and institutions in distinct issue-areas are evident in a large number of international processes, including: (1) the IANA function transition process and the broader review of ICANN accountability issues; (2) the World Internet Conference sponsored by China; (3) the NETmundial meeting and subsequent (controversial) "NETmundial Initiative"; (4) the decennial review of the World Summit on the Information Society (WSIS+10); (5) the UN GGE; (6) the Trans-Pacific Partnership (TPP) and Transatlantic Trade and Investment Partnership (TTIP); and (7) the UN Human Rights Council, Freedom Online Coalition and other attempts to protect rights online. These processes are characterized by increasing levels of contention. This contention has multiple causes, including path dependence, complexity and uncertainty, increasing distributional concerns and (in some cases) concerns about defection from cooperative agreements, and disagreement over legitimate procedural rules.[5] Disagreements over legitimate procedural rules for knitting formerly disparate regimes into a regime complex are especially noteworthy given the prevalence of debate over the nature and appropriateness of 'multistakeholder governance' as a mechanism for dealing with Internet issues. Advanced industrial democracies, members of the Shanghai Cooperation Organization and members of the G-77 have distinct views about how to legitimately engage in such processes. Internet issues are further complicated by the distinctive procedural expectations of the large firms that own most Internet infrastructure and of the Internet's technical community, composed primarily of engineers and computer scientists.[6]

Meeting these challenges entails accomplishing rule-making among scores of actors with diverse views of how to do it, with different conceptions of justice and different interests, amid complexity and uncertainty, and constrained by past choices. Under these conditions, it is virtually certain that actors will experience repeated, spectacular failures in their efforts to create and operate a cyber regime complex. However, humans are relatively resilient against failures of this kind; otherwise, maintaining large-scale, complex social systems would not be possible. We routinely get all kinds of things terribly wrong, and yet life goes on. But that does not mean failure is inconsequential. We can, and should, try to minimize failures and correct them quickly. To do so, governments and other relevant actors should do three things.[7] First, they should invest heavily in thinking and learning about desirable rules and procedures for managing cyber issues. In particular, efforts should be made in any policy development process to consider possible negative externalities of decisions for other related policy and governance areas. Such efforts need to be at least on the scale of learning processes created in the early nuclear period, which was the last time governments sought to deal with the implications of a fundamentally disruptive technological advance. Second, actors should seek to create a procedural *modus vivendi*. Here, the emphasis needs to be on explicit discussion of procedural, rather than merely substantive, issues. One example would be a mechanism for determining which forum should deal with a particular issue, as well as for deciding whether a new process or institution is required. Another example would be consideration of a dispute-settlement process explicitly concerned with reconciling conflicting requirements generated by different parts of the broader regime complex. Ensuring these procedural needs are met in a manner regarded as legitimate by various actors will be difficult, but cannot be neglected if the regime complex is to operate successfully. Third, and finally, it is vital that actors remain patient and inculcate an expectation of repeated failure and iteration.

Governance issues are central to the ways in which cyber-conflict is evolving and will continue to evolve.

Given its global, multistakeholder and highly-privatized nature, it would be unrealistic to propose the creation of a single new organization or process to address these and other challenges in the global cyber regime complex. It would be similarly unrealistic and also inappropriate to recommend militarizing or securitizing [8] the cyber regime complex in order to ensure the proper engagement of security and intelligence practitioners. Nevertheless, involving these parties is vital to ensuring the effectiveness and legitimacy of this regime complex. The next section of this article outlines the high stakes and some considerable difficulties in involving the military and intelligence communities in the cyber regime complex. It then argues that such efforts must begin at the cultural and attitudinal levels within the security and intelligence communities, and identifies four such attitudes. The section concludes by acknowledging some promising (though incomplete) efforts on the part of security and intelligence practitioners to engage with the broader cyber regime complex.

Engaging Security and Intelligence Practitioners in the Cyber Regime Complex

The primary reason to include the military and intelligence communities in the operation of the cyber regime complex is that they affect its viability and effectiveness. Security and intelligence practitioners have had, and will continue to have, both positive and negative effects on the broader global cyber regime complex. Security and intelligence practitioners are vital to ensuring a safe online environment for critical infrastructure, e-government and e-commerce. Despite high rates of private ownership of critical Internet infrastructure, governments play important roles in incident response and in ongoing cybersecurity education through the work of Computer Security Incident Response Teams (CSIRTs) such as the United States Computer Emergency Readiness Team (US-CERT). [9] The Cybersecurity Act of 2015 enhanced the US government's role in facilitating information-sharing about the existence and nature of cyber threats. [10] Government incentivizes improvements to hardware and software standards by exercising its buying power as a large procurer of information technology products and services. [11] Further, government officials continue to engage directly with key technical standard-setting bodies and with multistakeholder policy development processes concerning Internet issues, as well as with their counterparts in other governments. In this latter respect, they can make especially important contributions to stabilizing the rules of the road for state conduct in the cyber domain. [12] Insofar as security and intelligence practitioners succeed in these various tasks, they bolster the stability and interoperability of the global Internet and thereby facilitate the operation of the global cyber regime complex.

> Security and intelligence practitioners have had, and will continue to have, both positive and negative effects on the broader global cyber regime complex.

However, security and intelligence practitioners may also negatively impact the operation of the global cyber regime complex. Two such effects are particularly noteworthy. First, in the process of conducting intelligence, law enforcement or military operations they may deliberately or inadvertently (a) destroy Internet infrastructure and IT assets,[13] or (b) temporarily disrupt the normal operation of the Internet.[14] Second, they may also cause an erosion in trust by compromising (or attempting to compromise) Internet standards and technology, and by engaging in bulk data collection that is of dubious value in achieving national security objectives. Henry Farrell and Martha Finnemore have argued that the most significant damage caused by the Snowden revelations and similar leaks is a decrease in the ability of the US government to act hypocritically by simultaneously championing Internet freedom and maintaining extensive Internet monitoring.[15] Compounding the diplomatic damage from hypocrisy, former National Security Agency (NSA) official William Binneyhas suggested that these data collection programs are ineffective because they have inundated analysts with data.[16] This claim is supported, at least in the case of telephone metadata, by a White House review of NSA programs.[17]

It's likely impossible to entirely mitigate the negative effects of security and intelligence practitioners' activities on the global cyber regime complex.

James Comey, Director of the Federal Bureau of Investigation, has repeatedly advocated for a 'back door' into any encrypted communication.[18] This position has been publicly criticized by a group of leading technical experts, who suggest that it will undermine cybersecurity because of the difficulty in preventing unauthorized actors from using the same kind of access and because it has the potential to allow governments to violate human rights.[19] Comey's position has recently been disavowed by the Attorney General, Loretta Lynch,[20] but given the secrecy surrounding intelligence practices it is unlikely that such reassurances will convince skeptics. To the extent that public officials with security and intelligence portfolioscontinue to discount privacy concerns, it is likely that the that the overall legitimacy of the global cyber regime complex and public trust in the cyber domain as a whole will continue to erode.

To minimize the damage caused by their activities, and to maximize the benefits they can provide, it is important that security and intelligence practitioners become more engaged in the global cyber regime complex. However, given the confidential nature of their activities, there will clearly be challenges in ensuring appropriate levels of communication between security and intelligence practitioners on the one hand, and the remainder of the emerging global cyber regime complex on the other hand. It is likely impossible to entirely mitigate the negative effects of security and intelligence practitioners' activities on the global cyber regime complex, just as it will be impossible to entirely avoid adverse effects on the global cyber regime complex arising from the activities of its other participants (economic regulatory agencies, firms, international organizations, etc.). However, some steps can be taken to make partial improvements. Some such steps can be taken unilaterally by security and intelligence practitioners, while others require coordination with the technology community and other members of the global cyber regime complex.

Efforts to involve security and intelligence practitioners more effectively in the global cyber regime complex must begin at the cultural and attitudinal levels since organizational cultures and attitudes have broad and enduring effects on organizational behavior.[21] While cultural and attitudinal change may also be required in the private and voluntary sectors, I focus here on such changes within the security and intelligence communities. At its most basic, involvement in the global cyber regime complex need not entail official membership in organizations, speaking publicly on cyber issues or even attending meetings. The military and intelligence communities of advanced industrial democracies and emerging powers are undoubtedly watching these processes with more interest then they did even five years ago. Yet attention may not translate into positive outcomes. Ensuring that security and intelligence practitioners' activities have the most positive effects possible on the global cyber regime complex depends on substantial part on the attitudes adopted by such communities toward these governance processes. I focus on four attitudes that can be influenced by leaders within the military and intelligence communities, and that can help to minimize the chance of problematic interactions between security agencies and other parts of the global cyber regime complex.

> It is especially incumbent on security and intelligence practitioners to internalize the importance of carefully weighing the potential costs of their activities on other specific actors, and on the broader public interest.

It is especially incumbent on security and intelligence practitioners to internalize the importance of carefully weighing the potential costs of their activities on other specific actors, and on the broader public interest. The secrecy of their operations reduces (and often eliminates) opportunities for external review of the cost-benefit calculations made on such issues. For example, it is virtually impossible for such agencies to consult broadly with independent human rights experts and even with independent technical experts on the possible effects of a particular kind of cyber tool. More effectively internalizing effects on other parties requires being acutely aware that when different communities speak of cybersecurity; they often mean different things. Referent objects of the term ‘cybersecurity’ include the security of the physical network and of computer protocols, the security of critical national infrastructure, the security of intellectual property, and the security of users’ private information and other human rights. All of these perspectives need to be considered before reaching the conclusion that a particular kind of operation provides a net benefit.

Second, it is necessary for security and intelligence practitioners to resist the tendency to think of cyber operations as cheap or even costless. What may appear easy and cheap in the short-term may be costly in the long-term. This kind of concern is especially salient for early adopters of cyber technologies for military and intelligence purposes. Military use of such tools, as in the Stuxnet case, may encourage proliferation of such capabilities, as well as permissive international norms regarding their use. While recent work by the United Nations (UN) Group of Governmental Experts (GGE) indicates the possible emergence of basic norms for state conduct in the cyber domain,[22] contrary state practice could undermine such efforts. The other side of this coin is that if strong international norms do emerge in this area, militaries that invest heavily in such capabilities may be stuck holding devalued investments. Initially attractive intelligence programs may also turn out to be more costly in the long-run; this kind of dynamic is central to Farrell and Finnemore’s argument about the costs of hypocrisy. The corrosive effects of the Snowden revelations on the cyber regime complex, and on American diplomacy more broadly, are evident.[23] While this point is related to the previous point about ensuring that costs borne by other actors are internalized in calculations of costs and benefits undertook by security and intelligence practitioners, it bears mentioning to highlight the real possibility those other actors may attempt to reimpose the costs of negative externalities on those that generate them.

Military use of such tools, as in the Stuxnet case, may encourage proliferation of such capabilities, as well as permissive international norms regarding their use.

Third, it is important to resist the tendency to think of the Internet solely as a source of threat; such over-securitization carries real costs in terms of diminished openness and interoperability, and potentially also regarding stability. The risks of framing issues in concerning security has been recognized in diverse areas of IR scholarship since very shortly after the end of the Cold War prompted a rethinking of what we mean when we invoke the phrase ‘international security.’ Daniel Deudney argued that reframing environmental issues in terms of security might have problematic consequences.[24]

More recently, Stefan Elbe has pointed out that securitizing the challenge of HIV/AIDS likewise poses important ethical dilemmas.[25] Lene Hansen and Helen Nissenbaum have raised these issues directly in the context of cybersecurity. They argue that “the most significant lesson” of applying securitization theory to the cyber domain is that it highlights “the political and normative implications” of employing the cybersecurity frame. They conclude that “cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized and from the political to the technified”.[26] If cyber issues are prone to securitization, there is good reason to avoid further securitization at least until the issues are less novel and better understood. Securitization makes extraordinary steps (such as bulk Internet data collection) possible and diminishes opportunities for dissent or even policy review. It also contributes to a sense of urgency that may prompt rapid policy adoption that is inappropriate given the level of uncertainty about interactions between technologies and particular rule-sets.[27]

Finally, while each of these attitudes pertains to the way that security and intelligence practitioners make cost-benefit calculations in the course of fulfilling their missions, it is also important for these communities to take seriously the notion of appropriate limits on the means by which they accomplish their ends. In this regard, important current initiatives include those undertaken by various human rights bodies at the United Nations and by the GGE. The United Nations has affirmed that human rights are technologically neutral and that human rights apply online.[28] Accordingly, security and intelligence agencies are legally required to comply with their states’ respective human rights obligations. The GGE has concluded that the UN Charter applies online in its entirety, and also that the law of armed conflict applies in the digital domain.[29] This suggests that states have international obligations to respect the sovereignty of other states, as well as to refrain from intentional targeting of (and disproportionate damage to) civilian facilities and infrastructure. In the last three years, the rules of the road for state conduct in the cyber domain have become far clearer. Security and intelligence professionals can, therefore, engage productively with the global cyber regime complex by carefully considering the implications of these developments for their work and determining how best to accomplish their missions within these limits.

Despite the sensitive nature of their work, security and intelligence community members have found ways to engage more closely with parts of the global cyber regime complex. Much of this engagement is with private actors and is segmented primarily on national lines. Speculation exists regarding close ties between such agencies and various proxies in China, Russia, and other states.[30] Connections between US intelligence agencies and Silicon Valley firms have also been documented.[31] Governments have also engaged more closely with the Internet Corporation for Assigned Names and Numbers (ICANN), especially through its Governmental Advisory Committee (GAC), and with other technical bodies engaged in various aspects of Internet governance. However, such relationships typically involve government employees drawn from areas other than the military and intelligence communities.

The UN GGE remains a valuable mechanism allowing major governments to clarify their understandings of how international law applies in the cyber domain. While this work has addressed important questions of direct relevance to security and intelligence practitioners, the GGE cannot provide a sufficient venue for resolving problematic interactions between the military and intelligence communities and other parts of the cyber regime complex. First, the GGE is multilateral rather than multistakeholder in nature and thus does not provide effective means to coordinate with non-state actors. Second, it includes only a small number of governments, and enlarging it substantially risks undermining its ability to reach consensus. Third, it is an ad hoc body intended to foster dialogue on cyber norms, not to provide an ongoing facility for conflict resolution between elements in the broader global cyber regime complex.

Such mechanisms may be necessary for the long-run, but are unlikely to be created in the near future due to the complexity of creating such mechanisms among an array of heterogeneous actors with low levels of trust and high levels of uncertainty.[32] However, more modest outreach efforts to increase communication between security and intelligence practitioners and other parts of the cyber regime complex are both possible and desirable. As much as possible, these efforts should avoid strict segmentation on national lines, since coping with the potential for unintended transnational consequences is an important objective. Accordingly, states might pursue such outreach and engagement initiatives among preexisting regional and other groupings, to minimize trust problems. It is also advisable to begin by focusing on relations with academic experts. Such experts do not have the same profit motives and other incentives as private firms and even technical bodies, while they offer many of the same technical skills. The academics also include skill sets in law, policy, governance, and ethics that may be underrepresented in the private sector yet critical to improving the engagement of security and intelligence practitioners with the global cyber regime complex. Finally, military establishments often have substantial past experience in consulting with academics, for example on issues of nuclear strategy.[33] In managing such relationships, it is important for both sides to guard against outside experts being co-opted by security agencies, as such outcomes diminish the quality of the advice provided.

> The United Nations has affirmed that human rights are technogically neutral, and that human rights apply online.

This article concludes by advancing modest next steps for engaging security and intelligence practitioners with the global cyber regime complex, with the goal of minimizing the problematic interactions created by their work for other components of this vital part of contemporary global governance. These proposals are by no means exhaustive. They also, cannot be expected to eliminate problems for the effectiveness and legitimacy of the cyber regime complex arising from the work of military and intelligence agencies. Rather, they are intended to assist in minimizing such effects and in responding to them productively.

CONCLUSION

Security and intelligence agencies should continue (and, where possible, expand) their outreach efforts. Personnel from military cyber units and intelligence agencies could benefit from secondment not only to allied counterparts and technology firms, but also to think tanks, digital rights advocacy groups, and universities. Similarly, there are potential gains from fellowship programs that allow experts from academia and industry to spend time in security agencies. Initiatives such as the Army Cyber Institute at West Point indicate that the US government has begun to create such mechanisms, but it is important to ensure that such programs are broad in scope, adequately resourced, and coordinated across the many different service branches and civilian agencies with cyber capabilities. Deepening whole-of-government coordination on Internet governance files will also ensure the inclusion of views from the security and intelligence community in national positions and better inform security professionals on developments in the cyber regime complex.[34] The two-way nature of these efforts is vital to their utility. Security and intelligence practitioners must remain open to learning not only about efficiency improvements in their work but also about limits on their tools and their organizational cultures intended to safeguard Internet stability and interoperability.

Second, militaries and intelligence agencies should ensure that they institutionalize the capability to engage in good-faith troubleshooting when their activities cause unintended negative consequences for third parties. This recommendation is consistent with the suggestion for the development of an ‘e-SOS’ function for the cyber domain and an international legal duty to assist or responsibility to troubleshoot.[35] Given security sensitivities, this may require working with affected parties at arm’s length, likely through a national CSIRT. Absent some coordinating mechanism, CSIRTs and security agencies may find themselves working at cross-purposes. Coordination may not be feasible with especially sensitive programs and operations, but such conflicting efforts should be avoided where possible. Since such cases are likely to be among the most serious cyber disruptions given state capabilities, improving response quality will likely also improve the effectiveness and thus the legitimacy of the global cyber regime complex.

Third, security and intelligence agencies should institutionalize the responsibility to actively consider the effects of their policies, programs, and operations both on specific third parties and on the global public interest. This should be done by mandating the formation and genuine empowerment of teams of individuals trained to evaluate such impacts. These teams should consist of individuals with expertise in relevant technological fields as well as in law, ethics, politics, economics and international affairs. Their operation would closely parallel the role of so-called "Red Teams" in military planning.[36] For this reason, I suggest referring to them as "Green Teams" to emphasize their non-adversarial purpose, and to distinguish them from teams focused on strategically anticipating adversaries' reactions. While at least some portions of the US security and intelligence communities already attempt to consider such issues in their decision-making processes, it is important that such teams be empowered so that they can operate independently and make themselves effectively heard. Such considerations will become even more important over time given that the maturation of cyber technologies and cyber doctrines are likely to result in cyber capabilities being diffused throughout military force structures (rather than concentrated in the hands of special purpose elements) and perhaps even automated such that certain capabilities may be triggered without human action.

Finally, states that are early adopters of cyber capabilities in the security and intelligence communities should strive to ensure that all of the foregoing recommendations are adopted by any subsequent state that develops significant cyber capacity. This is especially important with respect to the formation and empowerment of Green Teams. The use of Green Teams should be regarded as analogous to the robust control systems created to safeguard against the accidental use of nuclear weapons. Just as states recognize a continuing interest in ensuring that any new nuclear powers adopt the best available safeguards,[37] there should be a recognition that all states share a similar interest in the development of restraint on the use of many cyber tools.

The increasing density and complexity of institutions for global governance are likely to generate further connections between efforts to govern different policy issues. Given the centrality of modern information and communications technologies to various areas of social, political and economic life, the cyber regime complex is certain to occupy a position of network centrality in this system, with connections to many other kinds of institutions. As a result, problematic interactions can be expected to be both relatively frequent and consequential. Mechanisms to manage these problematic interactions should, therefore, be a major priority, in the interest of minimizing damage to the effectiveness and legitimacy of the global cyber regime complex on which the stability and interoperability of the Internet depends. Security and intelligence practitioners have an important role to play in supporting the development of such mechanisms. They can, and should, take steps along the lines recommended in this article in order to minimize the chance that their work negatively affects the operation of the global cyber regime complex and of the global communications facilities that it supports.

NOTES

[1] Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs* International Engagement on Cyber III (2013a).

[2] The classic definition of a regime is found in Stephen D. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," *International Organization* 36.2 (1982), 185.

[3] Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series,* Paper No. 1 (2014). Available at https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

[4] Amandine Orsini, Jean-Frédéric Morin and Oran Young, "Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance," *Global Governance* 19.1 (2013).

[5] Timothy Simcoe, "Standard Setting Committees: Consensus Governance for Shared Technology Platforms," *American Economic Review* 102.1 (2010); Mark Raymond and Gordon Smith, "Reimagining the Internet: The Need for a High-Level Strategic Vision for Internet Governance," in Raymond and Smith (eds.), *Organized Chaos: Reimagining the Internet* (Waterloo: Centre for International Governance Innovation, 2014); Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond, "The Emergence of Contention in Global Internet Governance," Global Commission on Internet Governance Paper Series, No. 17 (Waterloo: Centre for International Governance Innovation, 2015). Available at https://www.cigionline.org/publications/emergence-of-contention-global-internet-governance.

[6] Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7.3 (2015).

[7] Mark Raymond, "Meeting Global Demand for Institutional Innovation in Internet Governance," in Roland Paris and Taylor Owen (eds.), *The World Won't Wait: Why Canada Needs to Rethink its International Policies* (Toronto: University of Toronto Press, 2016).

[8] Securitization refers to a process of socially constructing a particular issue as an existential threat to a valued referent object, in order to motivate action that may not be politically possible absent this framing. See Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner, 1998).

[9] See https://www.us-cert.gov/.

[10] See https://www.congress.gov/bill/114th-congress/senate-bill/754.

[11] Jeffrey Hunker, "U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away," *Journal of National Security Law and Policy* 4.1 (2010), 210.

[12] United Nations General Assembly A/70/174 (2015).*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement (accessed January 17, 2016).

[13] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53.1 (2011).

[14] Anita R. Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict," Journal of Peace Research 52.3 (2015); Philip N. Howard, Sheetal D. Agarwal and Muzammil M. Hussain, "When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media," *The Communication Review* 14.3 (2011).

[15] Henry Farrell and Martha Finnemore, "End of Hypocrisy: American Foreign Policy in the Age of Leaks," *Foreign Affairs* 92.6 (2013).

[16] Zack Whittaker, "NSA is So Overwhelmed with Data, it's No Longer Effective, Says Whistleblower," *ZDNet* (April 30, 2015). http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/ (accessed January 22, 2016).

[17] John Terbush, "Is the NSA's Data Snooping Actually Effective? *The Week* (December 19, 2013). http://theweek.com/articles/453981/nsas-data-snooping-actually-effective (accessed January 22, 2016).

[18] Nicole Perlroth and David E. Sanger, "F.B.I. Director Repeats Call That Ability to Read Encrypted Messages is Crucial," *New York Times* November 18, 2015. http://www.nytimes.com/2015/11/19/us/politics/fbi-director-repeats-call-that-ability-to-read-encrypted-messages-is-crucial.html (accessed January 22, 2016).

NOTES

19. Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," Computer Science and Artificial Intelligence Laboratory Technical Report (Cambridge MA: Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, (July 6, 2015). http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8 (accessed January 22, 2016).

20. Jeff Stone, "Loretta Lynch: US is Not Seeking Backdoor Access to Encrypted Communication but Wants Silicon Valley's Help," *International Business Times* (January 22, 2016). http://www.ibtimes.com/loretta-lynch-us-not-seeking-backdoor-access-encrypted-communication-wants-silicon-2276297 (accessed January 22, 2016).

21. See, for example, Peter J. Katzenstein (ed.), *The Culture of National Security* (New York: Columbia University Press, 1996). For an exploration of the ways in which organizational culture can become pathological, see Michael N. Barnett and Martha Finnemore, "The Politics, Power, and Pathologies of International Organizations," *International Organization* 53.4 (1999): 699-732. For a cautiously optimistic approach to employing such culture in explaining behavior, see Alistair Iain Johnston, "Thinking About Strategic Culture," International Security 19.4 (1995), 32-64.

22. UNGA (2015).

23. See also Bradshaw et al. (2015).

24. Daniel Deudney, "The Case Against Linking Environmental Degradation and National Security," *Millennium* 19.3 (1990).

25. Stefan Elbe, "Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security," *International Studies Quarterly* 50.1 (2006).

26. Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53.4 (2009), 1172.

27. On the desirability of flexible, soft law rule-sets in situations of high uncertainty, see Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54.3 (2000), 441-444.

28. United Nations General Assembly A/Res/68/167 (2013). *The Right to Privacy in the Digital Age.* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed January 25, 2016).

29. UNGA (2015).

30. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (2013). http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed January 29, 2016). See also: Ronald Deibert and Rafal Rohozinski, "Control and Subversion in Russian Cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* eds. Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (Cambridge: MIT Press, 2010).

31. James Risen and Nick Wingfield, "Web's Reach Binds N.S.A. and Silicon Valley Leaders," *New York Times* (June 19, 2013). http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=0 (accessed January 29, 2016).

32. Barbara Koremenos, Charles Lipson and Duncan Snidal, "The Rational Design of International Institutions," *International Organization* 55.4 (2001); Mark Raymond, "Renovating the Procedural Architecture of International Law," *Canadian Foreign Policy Journal* 19.3 (2013b); Raymond and DeNardis (2015).

33. Joseph S. Nye, Jr., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5.4 (2011).

34. Alexander Klimburg has called for the adoption of a 'whole of nation' approach, including firms and civil society, consistent with the more inclusive approach I call for in this article. See Alexander Klimburg, "Mobilising Cyber Power," *Survival: Global Politics and Strategy* 53.1 (2011).

35. See: Duncan Hollis, "An 'e-SOS' for Cyberspace," *Harvard International Law Journal* 52.2 (2011); Mark Raymond, "Managing Decentralized Cyber Governance: the Responsibility to Troubleshoot," Strategic Studies Quarterly 10.4 (forthcoming December 2016).

36. Gregory Fontenot, "Seeing Red: Creating a Red-Team Capability for the Blue Force," *Military Review* 85.5 (2005).

37. Adam M. Scheinman, "Calling for Action: The Next Generation Safeguards Initiative," *The Nonproliferation Review* 16.2 (2009).

Darknet Mining and Game Theory for Enhanced Cyber Threat Intelligence

John Robertson, Ahmad Diab, Ericsson Marin, Eric Nunes,
Vivin Paliath, Jana Shakarian, Paulo Shakarian [1]
Arizona State University

ABSTRACT

Due to a recent increase in popularity, Darknet hacker marketplaces and forums now provide a rich source of cyber threat intelligence for security analysts. This paper offers background information on Darknet hacker communities and their value to the cybersecurity community before detailing an operational data-collection system that is currently gathering over 300 threat warnings per week, with a precision of around 90% (Nunes 2016). Additionally, we introduce a game theoretic framework designed to leverage the exploit data mined from the Darknet to provide system-specific policy recommendations. For the framework, we provide complexity results, provably near-optimal approximation algorithms, and evaluations on a dataset of real-world exploits.

2. INTRODUCTION

The term "Darknet" refers to the anonymous communication provided by crypto-networks like "Tor". Contrast this definition with that of "Deepnet," which commonly refers to those sites hosted on the open portion of the Internet (i.e. the "Clearnet"), but are not indexed by search engines (Lacey 2015). Library catalogs and corporate websites for internal company use are good examples of deepnet presences.

Many corporations and government agencies rely on extensive penetration testing to assess the security of their computer networks. In a penetration test, a red team is hired to expose major flaws in the organization's security infrastructure. Recently, however, the market for exploit kits has continued to evolve, and what was once a rather hard to penetrate and exclusive market, whose buyers were primarily western governments (Shakarian 2013), has now become more accessible to a much wider population. Specifically, the Darknet portions of the internet is accessible through anonymization

John Robertson is a student at Arizona State University pursuing undergraduate degrees in both Computer Science and Electrical Engineering. He is the recipient of an Army Research Office Undergraduate Research Apprenticeship Program (ARO URAP) grant as well as two Fulton Undergraduate Research Initiative (FURI) grants for his work involving the application of artificial intelligence techniques to cyber-security problems in the Cyber-Socio Intelligent System (CySIS) Laboratory with Dr. Paulo Shakarian. For his work, John was nominated for the Computing Research Association's Outstanding Undergraduate Researcher award by the Computer Science faculty at ASU. John also has industry experience as a software engineering intern with Microsoft on the Windows Core Development team.

Ahmad Diab is a Computer Engineering Ph.D. student at Arizona State University. His current work in the Cyber-Socio Intelligent System (CySIS) Laboratory focuses on the application of artificial-intelligence techniques to cyber-security problems. Ahmad is a recipient of SIPGA award from ASTAR agency, Singapore. Previously, he was a Java developer at EtQ compliance Company. Ahmad holds a B.S. in computer engineering from Jordan University of Science and Technology (JUST).

Ericsson Marin is a Computer Science Ph.D. Student at Arizona State University. He works at the Cyber-Socio Intelligent System (CySIS) Laboratory under the guidance of Dr. Paulo Shakarian, with research projects in the intersection of Social Network Analysis (SNA), Artificial Intelligence (AI) and Cyber-Security. He received his MSc in Computer Science from Federal University of Goias, Brazil, and has published numerous papers in the area of social network analysis. He also holds a BSc in Computer Science and a Specialization in Software Quality and Management from Pontifical Catholic University of Goias, Brazil. He also has a real world experience as software designer managing different software factories. In 2015, Ericsson was awarded with a Brazilian Science Without Borders scholarship to pursue his Ph.D.

Vivin Paliath is a Computer Science Ph.D. student at Arizona State University. His research at ASU focuses on the application of artificial intelligence and game-theoretic techniques to cyber security problems. Vivin received both his B.S. in Computer Engineering and M.S. in Computer Science from Arizona State University. He has over a decade of industry experience and is also currently working as a Senior Software Engineer at Infusionsoft, a company that develops marketing-automation software for small businesses.

Jana Shakarian is a research scientist at Arizona State University and has been researching malicious hacking groups and their online activity since 2012. She has co-authored two books, Elsevier's *Introduction to Cyber-Warfare* and Springer's C*omputational Analysis of Terrorist Groups: Lashkar-e-Tabia.* She holds an M.A. in Sociology and Cultural and Social Anthropology from the Johannes Gutenberg University, Mainz, Germany. Previously, she worked as a staff social scientist for the University of Maryland Institute for Advanced Computer Studies (UMIACS) where she worked on major projects funded by the U.S. Air Force and Lockheed Martin.

Paulo Shakarian is an Assistant Professor at Arizona State University's School of Computing, Informatics, and Decision Support Engineering where he directs the Cyber-Socio Intelligent System (CySIS) Laboratory- specializing in cyber-security, social network analysis, and artificial intelligence. He has written numerous articles in scientific journals and has authored several books, including Elsevier's *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* His work has been featured in the major news media such as *The Economist, Popular Science,* and *WIRED.* He is a Cybersecurity Fellow with New America, a recipient of the Air Force Young Investigator Award, MIT Technology Review's "Best of 2013", and the DARPA Service Chiefs' Fellowship. Paulo also has won grant awards from ARO, ONR, DARPA, and others. Previously, Paulo was an Assistant Professor at West Point. Paulo holds a Ph.D. and M.S. in computer science from the University of Maryland, College Park, and a B.S. in computer science from West Point (with a Depth of Study in Information Assurance).

protocols such as Tor and i2p, which are now populated with multiple markets specializing in such products (Shakarian 2016; Ablon 2014). In particular, 2015 saw the introduction of Darknet markets specializing in zero-day exploit kits—exploits designed to leverage previously undiscovered vulnerabilities. These exploit kits are difficult and time-consuming to develop and often sold at premium prices, at times exceeding tens of thousands of dollars in cost. The widespread availability of zero-day exploits represents a potential game changer for penetration testers, specifically posing the following questions:

- *How can we automatically mine for new exploits and malware for sale in the malicious hacking community?*
- *What exploits will an attacker likely purchase if he targets a specific organization?*
- *What software used in the organization pose the biggest risk to new threats?*

However, the high cost of a variety of exploits available on the Darknet may preclude a penetration tester from simply obtaining them. In this paper, we present initial work that highlights steps toward solving these problems. To address the first question, we explore Darknet exploit markets and hacker forums through a data collection system to scrape, parse, and filter the web data. This data is then used as input to a novel, data-driven security game framework to address the second two questions. Specific contributions of this work include the following.

- A description of a system for automatically crawling and parsing Darknet malicious hacking information.
- A game-theoretic framework that, given a system configuration (or a distribution of system configurations within an organization) models an attacker as an agent who, with a finite budget, will purchase exploits to maximize his level of access to the target system. Likewise, a defender will look to adjust system configurations in an effort to minimize the effectiveness of an attacker while ensuring that necessary software dependencies are satisfied.
- A thorough formal analysis of the problems in the game-theoretic framework, including computational complexity results and approximation algorithms to identify provably near-optimal strategies for both players.
- A suite of experimental results on a prototype system that implements our game theoretic framework to demonstrate the effectiveness of this approach.

Paper organization. This paper's organization is as follows. Section 3 presents background information about the Darknet and the exploit marketplaces, and hacker forums that preside on the Darknet. Section 4 then details a data collection system for scraping and parsing these Darknet communities, including some of the technical challenges involved with utilizing such a system to provide up-to-date cyber threat intelligence. Section 5 includes a game theory framework, which mathematically formalizes problems for both the Attacker and Defender in a cyberattack scenario, along with complexity results and approximation algorithms for the framework. Finally, Section 6 presents the results of applying our framework on real-world Darknet exploits.

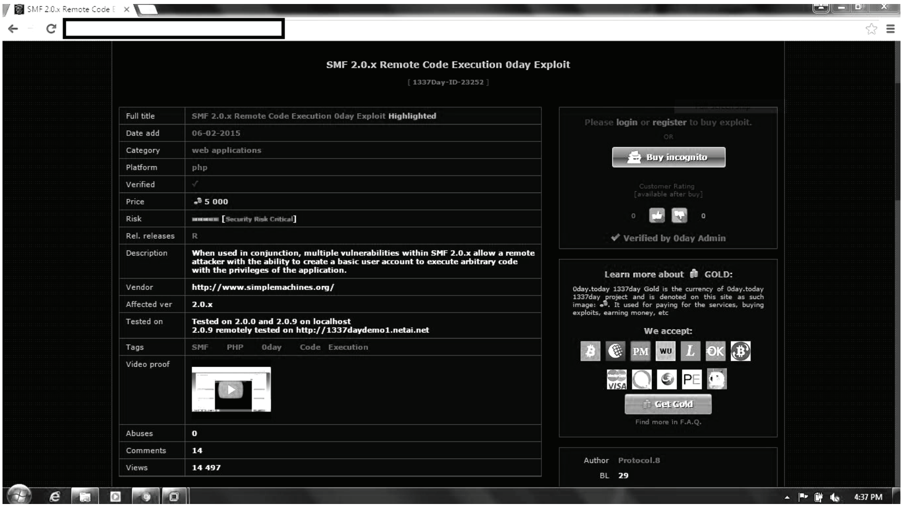
3. BACKGROUND

There are now a number of online communities providing users with both the ability to stay anonymous and the ability to reach geographically dispersed collaborators. As an illustration of the activity occurring on these communities, consider the exploit *MegalodonHTTP* Remote Access Trojan (RAT), which utilize the amateur black hat platform, HackForum, to facilitate its distribution. Five people accused of the malware's creation and/or distribution resided in three separate European countries, requiring law enforcement to cooperate internationally in pursuit of the malicious hackers'arrest (Wei 2013).

Darknet hacker marketplaces and forums now provide a rich source of cyber threat intelligence for security analysts.

Darknet and Deepnet Sites. Widely used for underground communication, *The Onion Router* (Tor) is free software designed to protect the privacy of its users by obscuring traffic analysis, greatly complicating network surveillance (Dingledine 2004). The network traffic in Tor flows through a number of volunteer-operated servers (also called *nodes*). Each node of the network encrypts the information it blindly passes on, neither registering where the traffic came from nor where it is headed (Dingledine 2004). Effectively, this allows not only for anonymized browsing (the IP address revealed will only be that of the exit node), but also for circumvention of censorship.[2]

These online hacker communities may take on a number of different forms. We discuss a few below.



[redacted]

SMF 2.0.x Remote Code Execution 0day Exploit

[1337Day-ID-23252]

Full title	SMF 2.0.x Remote Code Execution 0day Exploit **Highlighted**
Date add	06-02-2015
Category	web applications
Platform	php
Verified	✓
Price	5 000
Risk	[Security Risk Critical]
Rel. releases	R
Description	When used in conjunction, multiple vulnerabilities within SMF 2.0.x allow a remote attacker with the ability to create a basic user account to execute arbitrary code with the privileges of the application.
Vendor	http://www.simplemachines.org/
Affected ver	2.0.x
Tested on	Tested on 2.0.0 and 2.0.9 on localhost 2.0.9 remotely tested on http://1337daydemo1.netai.net
Tags	SMF PHP 0day Code Execution
Video proof	
Abuses	0
Comments	14
Views	14 497

Please **login** or **register** to buy exploit.

OR

Customer Rating
[available after buy]

0 0

✓ Verified by 0day Admin

Learn more about GOLD:

0day.today 1337day Gold is the currency of 0day.today 1337day project and is denoted on this site as such image: . It used for paying for the services, buying exploits, earning money, etc

We accept:

Find more in F.A.Q.

Author Protocol.8

BL 29

Figure 3.1: Example of Darknet Market

Markets. Darknet marketplaces provide users with a platform for buying and selling illicit merchandise. Common products include drugs, weapons, pornography, and exploits. Figure 3.1 depicts listings for zero-day exploits on one such market. These markets contain rich information about the cyber threat landscape; though commonly only a small fraction of products (12.6% in our collected data to date) are related to malicious hacking. Vendors often advertise their products on non-market communities (e.g. forums) to attract attention towards their goods and services. To facilitate transactions, marketplaces often have a wallet in which users will deposit digital currency, though sometimes administrators will serve as an escrow service. Products are most often verified before any funds are released to the seller, and if a seller is misleading or fails to deliver the appropriate item, they can be banned from the site. Similarly, buyers can be banned for not complying with site-specific transaction rules.

Forums. Forums are user-oriented platforms that have the sole purpose of enabling communication. They provide the opportunity for the emergence of a community of like-minded individuals, regardless of their geophysical location. To ensure user safety and privacy, forum administrators often incorporate different security mechanisms into the site. For example, during registration (though not necessarily with every login) every prospective member has to complete CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), answer simple questions, solve puzzles or complete simple arithmetic operations, presumably to prevent automated access. Discussion forums on the Darknet consist of boards and sub-boards (also called *child-boards*) filled with threads concerned with different topics (for example the discussion of a platform-specific vulnerability). While the structure and organization of Darknet-hosted forums might be very similar to the more familiar clearnet-forums, the discussion topics vary distinctly. In the English clandestine Darknet, people interested in cats, steampunk, and the latest conspiracy theories convene, but there is an abundance of arenas dedicated to child pornography (CP), drugs, and weapons. Lengthy threads seek information on the reliability of individual marketplace vendors, and the quality of specific marketplaces in general. As Darknet sites are typically not indexed by search engines (for example Google), frequently these forums will link to other Darknet sites and provide information on other potentially fraudulent websites. Forums concerning malicious hacking will feature discussions on programming and cybersecurity.

Subreddits. Reddit is a clearnet site that acts as a content aggregator where users can come together and form sub-communities focused on specific topics. These sub-communities are subreddits. Some subreddits, specifically the ones that are of interest to our research focus on the discussion of darknet exploit markets. Important information regarding the marketplace environment including reviews of marketplaces, products, and vendors are often discussed on these subreddits. These links and sentiments about markets can provide insight. For instance, we might learn to predict when popular opinion shifts with respect to a certain market. Subreddits also provide information concerning marketplaces and forums that are newly introduced or old ones that are shutting down.

> The widespread availability of zero-day exploits represents a potential game changer for penetration testers.

Tor-hosted platforms are often shorter lived than their clearnet counterparts. Darknet sites migrate frequently or alternate through multiple addresses, oftentimes resulting in unreliable availability (or uptime). Through search engines and spider services, which traverse links on the Darknet and aggregate the visited links in a list (similar in nature to a *Crawler* (Section 4.1)), on the Tor-network we were able to find more than sixty forums populated by malicious hackers. Other platforms were discovered through links posted on forums, either on the Tor-network or on the clearnet. About half of these forums use English to communicate (33), but French (8), Russian (4), Swedish (2), and (5) other languages were used. On the clearnet, we found more than seventy forums for black hat hackers, the majority of which are English-speaking (52), 18 are in Russian, and one each in French and Polish.

Related Work

Exploit markets on the Darknet. While Darknet criminal activity over the past decade has been extensively studied for issues such as drug trade (Soska and Christin 2015) and terrorism (Chen 2011), the markets of exploits existing on the Darknet are much less well understood. There has been related work on malicious hacker forums (Zhao et al. 2012;

Li and Chen 2014), which did not focus on the purchase and sale of specific items. Markets of malicious products relevant to cybersecurity have been previously studied (Ablon et al. 2014; Shakarian and Shakarian 2015), but none of these works gathered data on specific exploits (or other products) from either the darkweb or open Internet, nor did they examine the markets through the lens of security games. This work extends the initial results presented in (Robertson 2016) and further describes the collection of price data on specific exploits for sale on the deep web, consequently analyzing them in a security game framework to yield policy recommendations for cyber-defenders tailored for specific system configurations.

Darknet sites migrate frequently or alternate through multiple addresses, oftentimes resulting in unreliable availability.

Security games. In recent years, *security games* where attacker-defender models are used to inform the actions of defenders in military, law-enforcement, and homeland security applications have gained much traction; see (Tambe 2011) for an overview. With regard to cybersecurity, there have been many contributions including intrusion detection (Nguyen et al. 2009), attack graph based games (Lye and Wing 2005) and honeypot placement (Kiekintveld et al. 2015). However, to the best of our knowledge, (Robertson 2016), from which this work extends, represents the first game theoretic approach to host-based defense where the activities of the attacker are informed from an *unconventional* source (information not directly related to the defender's system)— specifically information from Darknet markets in this case. Further, the very recent emergence of Darknet markets specializing in zero-day exploits allows for the integration of information that was unavailable in previous work.

4. DATA COLLECTION

Table 4.1 demonstrates how these communities leverage for valuable cyber threat intelligence, which highlights the lifecycle of a vulnerability from identification to exploitation. FireEye, a major cybersecurity firm, identified that the Dyre Banking Trojan was designed to steal credit card information exploited this particular vulnerability, illustrating how threat warnings gathered from the Darknet can provide valuable information for security professionals. Between Dyre and the similar Dridex banking trojan, nearly 6 out of every 10 global organizations were affected, a shocking statistic.[3]

In another instance, 17-year-old hacker Sergey Taraspov from St. Petersburg, Russia, along with a small team of hackers, allegedly wrote a piece of malware that targeted point-of-sale (POS) software and sold it for $2,000 on a Russian forum/marketplace. This malware was, in turn, used by around forty individuals to steal over 110 million American credit card numbers in the *Target* data breach of 2013.[3]

Timeline	Event
February 2015	Microsoft identifies Windows vulnerability MS15-010/CVE 2015-0057 for remote code execution. There was no publicly known exploit at the time the vulnerability was released.
April 2015	An exploit for MS15-010/CVE 20150057 was found on a Darknet market on sale for 48 BTC (around $10,000-15,000).
July 2015	FireEye identified that the Dyre Banking Trojan, designed to steal credit card numbers, exploited MS15010/CVE 2015-0057[2].

Table 4.1: Exploit example.

To gather exploit information from these Darknet markets, we have assembled a sophisticated data pipeline whose system diagram is depicted in Figure 4.5. The technical challenges associated with this system will be briefly discussed in Section 4.1. This operational system currently collects over 300 cyber threats from Darknet markets each week. Figure 4.2 shows the cumulative count of detected threats for five weeks. Figure 4.3 shows a social network, which connects vendors across multiple marketplaces, built using the collected data. At the time of this writing, we are transitioning the system to a commercial partner. Table 4.4 depicts the current database statistics, including the total amount of data collected and the amount of hacking-specific data. The vendor and user statistics cited considers those individuals associated in the discussion or sale of malicious hacking-related material, as identified by our system. This data can address questions such as,

- *What vendors and users have a presence in multiple Darknet/deepnet markets/forums?*
- *What zero-day exploits are being developed by malicious hackers?*
- *What vulnerabilities do the latest zero-day exploits target?*
- *How can a system's presented attack surface be altered to reduce the potential damage of a cyberattack?*

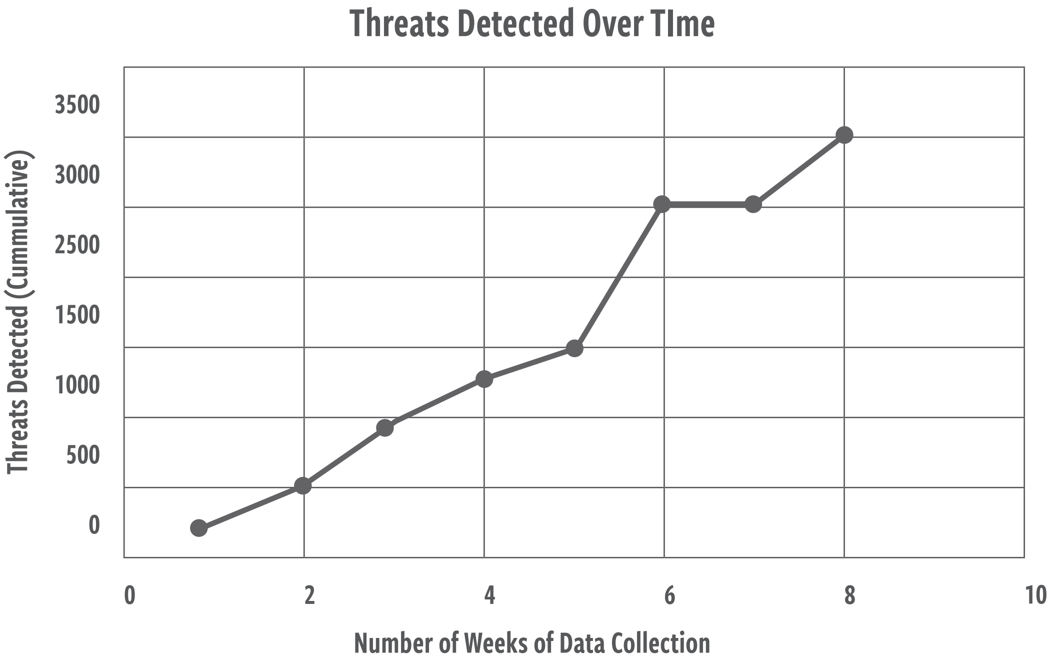


Figure 4.2: Weekly detection of cyber-threats.

Figure 4.3: Vendor network connecting vendors across multiple marketplaces

Markets	Total Sites Total Products	32 18682
	Hacking-Related	2934
	Vendors (Hacking-Related)	508
Forums	Total Number Total Topics/Posts	23 146053/263363
	Hacking-Related	29636/18392
	Users (Hacking-Related)	11025
Subreddits	Total Number Topics/Posts	33 3940/19601
	Hacking-Related	1654/8270

Table 4.4: Current Database Status

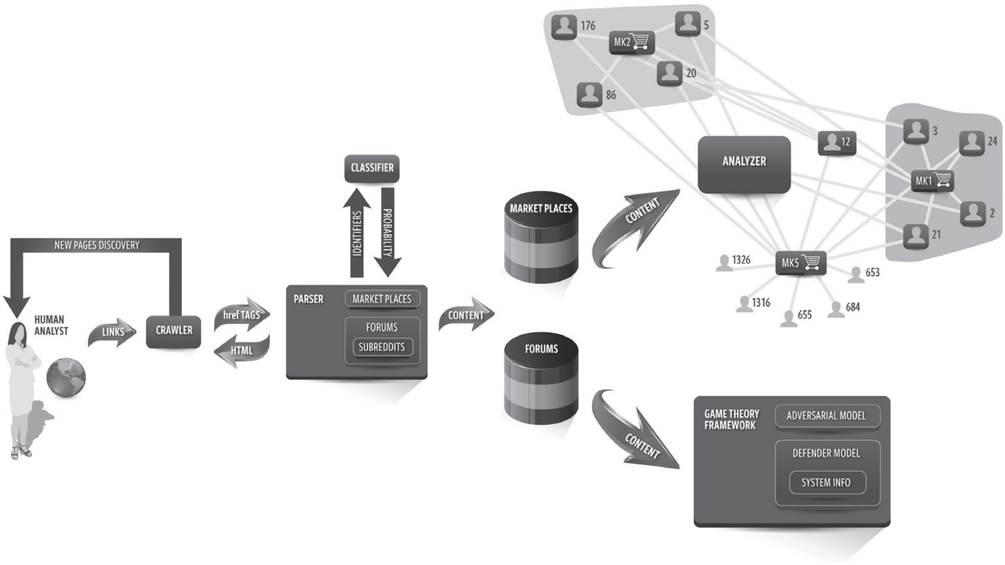


Figure 4.5: System Overview (see page 121 for an enlarged version of the diagram)

4. SYSTEM OVERVIEW

Figure 4.5 gives the overview of the system, whose components are described below.

Crawler. The crawler is a program designed to traverse through a website and retrieve its HTML documents. Topic based crawlers have been used for focused crawling where only webpages of interest are retrieved (Menczer 2004; Chakrabarti 1999). More recently, focused crawling was employed to collect forum discussions from the Darknet (Fu 2010). We have designed separate crawlers for different platforms (markets/forums) due to the structural difference and access control measures for each platform. Our crawler addresses technical challenges such as access control, unresponsive servers, duplicated links (which create a loop), etc., to gather information regarding products from markets and discussions on forums.

Parser. After downloading all html files from a given site, the pages are passed to a parser to extract specific information from marketplaces (e.g. price, vendor, listing date, etc.) and hacker forums (e.g. posts, participating users, etc.). This well-structured information can then be stored in a relational database. Due to idiosyncrasies with each site, typically a unique parser must be written for each site to extract the desired information. The parser also communicates with the crawler; that is, the parser communicates a list of relevant webpages to the crawler, which are then re-crawled to get time-varying data. For markets we collect the following important products fields: {item title, item description, vendor name, shipping details, item reviews, items sold, CVE, items left, transaction details, ratings}. For forums and subreddits we collect the following fields: {topic content, post content, topic author, post author, author status, reputation, topic interest}.

The very recent emergence of Darknet markets specializing in zero-day exploits allows for the integration of information that was unavailable in previous work.

Classifier. As mentioned previously, on these sites not all information is strictly related to cybersecurity and/or hacking. Because of this, it is useful to automate the process of classifying a given product or forum discussion as hacking-related or not. To that end, many data mining techniques are utilized to filter out any irrelevant (meaning not related to cybersecurity) products and discussions. In essence, we leverage a security analyst-labeled dataset with machine learning techniques to detect relevant products and topics from these sites, filtering out products and threads concerning drugs, weapons, and other material not relevant to malicious hacking. Additionally, we leverage topic modeling and other data mining techniques to expedite the process of new site discovery, see (Nunes 2016) for an overview of the machine learning techniques utilized.

Product	Price in BTC	Price in $*
GovRAT (Source Code + 1 Code Signing Certificate Included)	2.000	$456.92
0day Wordpress MU Remote Shell	1.500	$342.69
A5/1 Encryption Rainbow Tables	1.500	$342.69
Unlimited Code Signing Certificate	1.200	$274.16
Ready-made Linux botnet 600 SERVERS	1.200	$274.16
FUD version of Adobe Flash <=16.0.0.287 (CVE 2015-0311)	2.626	$600.00

*Price in U.S. Dollar on date of data collection (Sep. 1, 2015) [1 BTC = $228.46]. As of Aug. 21, 2016, the conversion rate is now [1 BTC = $580.87].

Table 4.6: Example of Products offered on Darknet Markets

5. GAME THEORETIC FRAMEWORK

Here we formalize the concept of our security game where the attacker is a malicious hacker with access to Darknet exploit markets, and the defender is tasked with host-based defense of either a single system or group of systems. We use the notation *V* to represent the entire set of vulnerabilities within a given computer system. Though there may be vulnerabilities not yet detected by the system administrator, we can mine for information on new vulnerabilities through an examination of Darknet hacking markets. In a real-world organization, system administrators are not able to patch all vulnerabilities for a variety of reasons. Software dependencies, use of legacy systems, and non-availability of patches are some examples. To model this, we define a *constraint set* (denoted C) as a subset of *V.* The vulnerabilities in a constraint set represent the vulnerabilities required for some system functionality. When each vulnerability in a constraint set C is in the presented attack surface (that is externally accessible), C is then said to be satisfied and the system supports the functionality modeled by C. Let **C** represent the set of all possible constraint sets. We extend this idea with an *application constraint set* which, for an arbitrary application, *i*, denoted $\mathcal{C}_i$, is a set of constraint sets (i.e $\mathcal{C}_i \subseteq \mathbf{C}$). Each constraint set in $\mathcal{C}_i$ represents a set of vulnerabilities that together will provide the complete functionality required of application *i.* $\mathcal{C}_i$ is said to be satisfied if any single constraint set in $\mathcal{C}_i$ is satisfied. If $\mathcal{C}_i$ is satisfied by a system configuration, and hence at least one constraint set in $\mathcal{C}_i$ is satisfied, application i will properly operate on the system. Then $\mathcal{C}$ is the set of all application constraint sets for a given system configuration and represents all of the applications to be run on the system. In this framework, for a given system, a system administrator must select which vulnerabilities must be present in order to allow each application i to function. This begs the question as to how to make this selection—so we now start to define some concepts relevant to the adversary.

We will use *ex* to denote a particular exploit—a technique used to take advantage of a given vulnerability. Let *Ex* denote the set of all possible exploits and **Ex** denote the set of all possible exploit sets (i.e. $\mathbf{Ex} = 2^{Ex}$). For each $ex \in Ex$, c_{ex} is the associated cost of exploit *ex*—and this is specified directly on a Darknet market (normally in Bitcoin). Associated with the set of exploits is the Exploit Function, *ExF,* which takes a set of exploits as input and returns a set of vulnerabilities (i.e. $ExF : \mathbf{Ex} \rightarrow 2^V$). The set of vulnerabilities produced by $ExF(A)$, for a given set of exploits A, represents the vulnerabilities that are exploited by the exploits in A. While many possible variations of an exploit function are possible, in this paper, we will use a straightforward definition that extends the exploit function from singletons (whose associated vulnerabilities can be taken directly from the online marketplaces) to sets of exploits: $ExF(A) = \bigcup_{a \in A} ExF(\{a\})$. For use in proving complexity results, we shall denote the special case where $Ex = V$, $ExF(A) = A$, and $\forall ex \in Ex, c_{ex} = 1$ as the *Identity Exploit Model*.

5.1 PLAYER STRATEGIES AND PAYOFF

An attacker will use a set of exploits to attempt to gain access to a system, and must do so within a budget. Likewise, the defender must identify a set of vulnerabilities that he is willing to expose (often referred to as the *presented attack surface*). We define strategies for the two players formally as follows.

Definition 5.1. *(Attack Strategy). Given budget $k_{atk} \in \mathbb{R}^+$, an Attack Strategy, denoted A is a subset of Ex such that $\Sigma_{a \in A}\, c_a \leq k_{atk}$.*

Definition 5.2. *(Defense Strategy). Given a family of application constraint sets $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \ldots \mathcal{C}_n\}$, a Defense Strategy, denoted D is a subset of V such that for each $\mathcal{C}_i \in \mathcal{C}$, there exists $\mathrm{C} \in \mathcal{C}_i$ where $\mathrm{C} \subseteq D$ (that is each application constraint is satisfied by D).*

Note that when a defense strategy D meets the requirements of $\mathcal{C}$, as per Definition 5.2, we say *D satisfies $\mathcal{C}$.* We will use the notation $\mathbf{A}, \mathbf{D}$ to denote the set of all attack and defense strategies, respectively, and refer to an attacker-defender pair of strategies as a *strategy profile.* We will also define a *mixed strategy* for both players in the normal manner. For the attacker (respectively defender) a *mixed strategy* is a probability distribution over $\mathbf{A}$ (respectively $\mathbf{D}$). We shall normally denote mixed strategies as Pr_A, Pr_D for each player and use the notation $|Pr_A|$ (respectively $|Pr_D|$) to denote the number of strategies in $\mathbf{A}$ (respectively $\mathbf{D}$) that are assigned a nonzero probability by the mixed strategy. We now turn our attention to the payoff function, which we define formally as follows:

Definition 5.3. *(Payoff Function). A payoff function, p, is any function that takes a strategy profile as an argument and returns a positive real. Formally,*

$$p : \mathbf{A} \times \mathbf{D} \rightarrow \mathbb{R}^{+}$$

Unless noted otherwise, we will treat the payoff function as being computable in polynomial time. Also, the payoff function is underspecified—which is designed to allow flexibility in the framework. However, in the context of the results of this paper, we shall consider the following *payoff function axioms:*

$\forall D \in \mathbf{D}, \forall A \in \mathbf{A}$ such that $ExF(A) \cap D = \emptyset, p(A,D) = 0$	(1)
$\forall D \in \mathbf{D}, \forall D_0 \subseteq D, \forall A \in \mathbf{A}, p(A,D_0) \leq p(A,D)$	(2)
$\forall D \in \mathbf{D}, \forall A \in \mathbf{A}, \forall A_0 \subseteq A, p(A_0,D) \leq p(A,D)$	(3)
$\forall A \in \mathbf{A}, D, D_0 \in \mathbf{D}\ p(A,D) + p(A,D_0) \geq p(A, D \cup D_0)$	(4)
$\forall D \in \mathbf{D}, A, A_0 \in \mathbf{A}, p(A,D) + p(A_0,D) \geq p(A \cup A_0, D)$	(5)

Axiom 1 states that if the vulnerabilities generated by an attack strategy's exploits and the vulnerabilities in a defense strategy are disjoint sets, the payoff function must return 0. A consequence of axiom 1 is that if either the attack strategy or the defense strategy is the empty set, the payoff function will return 0. Axioms 2 and 3 require the payoff function to be monotonic in the size of the attack and defense strategies. Axioms 4 and 5 require the payoff function to be sub-modular with respect to the attack and defense strategies.

In this paper, we shall (in general) focus on the *overlap payoff function,* which we shall define as follows: $p(A,D) = |ExF(A) \cap D|$. Intuitively, this is simply the number of vulnerabilities exploited by the attacker. Further, when dealing with mixed strategies, we shall discuss payoff in terms of expectation. Expected payoff can be formally defined as follows:

$$Exp(Pr_A, Pr_D) = \Sigma_{D \in D}\, \Sigma_{A \in A}\, Pr_A(A)\, Pr_D(D)\, p(A,D)$$

Using the overlap function, the expected payoff can be interpreted as the *expected number of exploited vulnerabilities.*

5.2 PROBLEM FORMULATIONS

We now have the components to define a pair of decision problems dealing with the best response for the players. These problems are the deterministic host attacker problem (DHAP) and deterministic host defender problem (DHDP), respectively, and are defined as follows:

DHAP

INPUT: $k_{atk} \in \mathbb{R}^{+}$, $x \in \mathbb{R}^{+}$ mixed defense strategy Pr_D, and payoff function *p.*

OUTPUT: “Yes” if $\exists A \in \mathbf{A}$, such that $\Sigma_{a \in A}\, c_a \leq k_{atk,}$ and $\Sigma_{D \in D}\, Pr_D\,(D)\, p\,(A,D) \geq x$
“No” otherwise.

DHDP
INPUT: application constraints, mixed attack strategy Pr_A, and payoff function p.
OUTPUT: “Yes” if $\exists D \in \mathbf{D}$, such that $\Sigma_{A \in A}\, Pr_A\,(A)\, p(A, D) \leq x$ and D satisfies $\mathcal{C}$ and
“No” otherwise.

The natural optimization variants for these two problems will deal with maximizing the payoff in DHAP and minimizing the payoff in DHDP.

5.3 COMPLEXITY RESULTS

In this section, we analyze the complexity and limits of approximation for both DHAP and DHDP. We use the *Identity Exploit Model* for the complexity results. Unfortunately, both problems are NP-Complete in the general case.

Theorem 1. DHAP is NP-Complete, even when $|Pr_D| = 1$ and the payoff function adheres to the submodularity and monotonicity axioms.

Proof Sketch. Membership in NP is trivial if the payoff is PTIME computable. The hardness result relies on an embedding of the well-known budgeted set cover (Feige 1998). Here, the defender’s strategy is treated as a set of elements to cover and the exploits are treated as subsets of D (by virtue of the exploit function). Exploit costs are set as 1 and the attacker’s budget is the value budget from the embedded problem. So, the attacker must pick exploits to meet the budget and cover the determined number of the defender’s vulnerabilities.

Theorem 2. When $|\mathcal{C}| > 1$ and $|Pr_A| = 1$, DHDP is NP-Complete.

Proof Sketch. Again, membership in NP is trivial if the payoff is PTIME computable. Hardness is shown by embedding the hitting set problem. In this reduction, the attacker plays all exploits and each exploit corresponds with precisely one vulnerability. This has the effect of imposing a unit cost on each vulnerability. Here, each $\mathcal{C}_i$ must be covered by a vulnerability. Hence, the defender must pick a set of all vulnerabilities to meet the cost requirement of DHDP while covering each $\mathcal{C}_i$.

We are also able to analyze the hardness of approximation for the optimization variants of DHAP and DHDP. Because the above embedding’s used set cover and hitting set, we can draw upon the results of (Feige 1998) to obtain the following corollaries:

Corollary 3. DHAP cannot be approximated where the payoff is within a factor of $(1-\frac{1}{e})$ unless $P = NP$

Corollary 4. DHDP cannot be approximated where the payoff is within a factor of $(1 - o(1))ln(\mathrm{n})$unless $P = NP$

5.4 ALGORITHMS

Technical Preliminaries

Definition 5.3 *(Marginal Gain). Given a payoff function p and a mixed defense strategy* $Pr_{D,}$ $\Delta_{p,Pr_D}(a|A)$ *will measure the marginal gain of exploit a in the context of an attack strategy A. That is,* $\Delta_{p,Pr_D}(a|A) = \Sigma_{D\in Pr_D} p(A \cup \{a\}, D) - p(A, D)$

With the limits of approximation in mind, we can now introduce several algorithms to solve the optimization variants of DHAP and DHDP. The optimization variant of DHAP under the overlap payoff function is a special case of submodular maximization with the distinction that we are not simply picking *k* discrete objects, but instead picking items that each have a unique cost associated with them. Understanding this, we examine several different approaches to this problem based on the literature on submodular maximization. DHDP, on the other hand, can be readily approximated using the traditional set-cover algorithm (under some realistic assumptions), as cost does not affect DHDP.

Algorithm 1 Lazy Greedy Algorithm (Cost-Benefit Variant)

```
Input: $k_{atk} \in \mathbb{R}^+$, $Pr_D$, and payoff function $p$.
Output: $A \subseteq Ex$ such that $\Sigma_{a\in A} c_a \leq k_{atk}$
A ← ∅; cost ← 0; priority queue Q ← ∅; iter ← 1
for $e \in Ex$ do
    $e.key \leftarrow \frac{\Delta_{p,Pr_D}(e|\emptyset)}{c_e}$; $e.i \leftarrow 1$
    Insert e into Q with e.key as its key
end for
while $\{a \in Ex \backslash A : c_a + cost \leq k_{atk}\} \neq \emptyset$ do
    extract top (max) element e of Q
    if $e.i = iter$ and $c_e + cost \leq k_{atk}$ then
        $A \leftarrow A \cup \{e\}$; $iter \leftarrow iter + 1$
        $cost \leftarrow cost + c_e$
    else if $c_e + cost \leq k_{atk}$ then
        $e.i \leftarrow iter$; $e.key \leftarrow \frac{\Delta_{p,Pr_D}(e|\emptyset)}{C_e}$
        re-insert $e$ into Q
    end if
end while
return $A$
```

Algorithms for DHAP

Greedy Approaches. As mentioned earlier, the non-unit cost of exploits mean that DHAP can be considered as a submodular maximization problem subject to knapsack constraints. Two versions of the traditional greedy algorithm (Nemhauser 1978) can be applied: a cost-benefit variant and uniform-cost variant, both of which will also use the lazy-greedy optimization (Minoux 1978) to further enhance performance while maintaining the approximation guarantee. We note that independently, the uniform-cost and the cost-benefit algorithms can perform arbitrarily badly. However, by extending a result from (Leskovec 2015), either the cost-benefit or the uniform-cost algorithm will provide a solution within a factor of $\frac{1}{2}(1-\frac{1}{e})$ for a given set of input parameters. By applying both algorithms to a given problem instance and returning the attack strategy which produces the larger payoff, the $\frac{1}{2}(1-\frac{1}{e})$ approximation factor is achieved for DHAP. A cost-benefit lazy approximation algorithm is shown in Algorithm 1. By removing "C_e" from the denominator in the *e.key* assignment in lines 3 and 12, the cost benefit lazy approximation algorithm is transformed into a uniform cost lazy approximation algorithm.

Multiplicative Update Approach. An improved approximation ratio, when compared with the $\frac{1}{2}(1-\frac{1}{e})$ ratio for the greedy algorithms, can be obtained by adapting Algorithm 1 from (Azar and Gamzu 2012) for DHAP. This is shown as Algorithm 2 in this paper. For some value ϵ (a parameter), this algorithm provides a $(1-\epsilon)(1-\frac{1}{e})$ approximation of the optimal solution (Theorem 1.2 in (Azar and Gamzu 2012)), which, by providing an exceedingly small ϵ value, can get arbitrarily close to the $(1-1/e)$ optimal approximation limit we discussed earlier.

Algorithm 2 Multiplicative Update

Input: $k_{atk} \in \mathbb{R}^{+}$ such that $0 < \epsilon < 1$, Pr_D, and payoff function p.

Output: $A \subseteq Ex$ s.t. $\Sigma_{a \in A} c_a \leq k_{atk}$

```
$Ex' \leftarrow \{ex \in Ex : c_{ex} \leq k_{atk}\}$
$A \leftarrow \emptyset$
$W \leftarrow \min_{ex'_i \in |Ex'|} k^2_{atk} / C_{ex'_i}$
$w \leftarrow \frac{1}{k_{atk}}$; $\lambda \leftarrow e^{\frac{\epsilon W}{4}}$
**while** $k_{atk}{}^{w} \leq \lambda$ and $Ex' \neq \emptyset$ **do**
    $ex_j \leftarrow argmin_{exj \in Ex' \setminus A}(\frac{C_{ex_j}}{k_{atk}} w / \Delta_p, Pr_D (ex_j \mid A))$
    $A \leftarrow A \cup \{ex_j\}$
    $w \leftarrow w \lambda^{c_{exj} / k^2_{atk}}$
    $Ex' \leftarrow Ex' \setminus \{ex_j\}$
```

```
end while
if $\Sigma_{A_i \in A} c_{A_i} \leq k_{atk}$ then
    return $A$
else if $\Sigma_{D \in Pr_D} Pr_D\ (D)\, p\, (A \backslash \{ex_j\}, D) \geq \Sigma_{D \in Pr_D} Pr_D\ (D)\, p\, (\{ex_j\}, D)$ then
    return $A \backslash \{ex_j\}$
else
    return $\{ex_j\}$
end if
```

Algorithms for DHDP

When using the overlap payoff function, DHDP can be modeled as a weighted set cover problem. Because the overlap payoff function is a modular function, the associated cost of a given vulnerability v, is simply the payoff produced by the singleton set $\{v\}$ with a mixed attack strategy Pr_A i.e. $c_v = \Sigma_{A \in A} Pr_A\, (A)\ p\ (A, \{v\}$. In the common case where each constraint set is a singleton set (i.e. $\forall \mathcal{C}_i \in \mathcal{C}, \forall \mathrm{C} \in \mathcal{C}_i, |\mathrm{C}|=1$), if the overlap payoff function is used, an adaptation on the standard greedy weighted set cover algorithm can be used for DHDP (Algorithm 3), providing a $ln(n) + 1$ approximation (Feige 1998).

Algorithm 3 Weighted Greedy DHDP Algorithm for Singleton Constraint Set and Overlap Payoff Case

```
Input: Vulnerabilities $V$, $Pr_A$, and application constraints $\mathcal{C}$
Output: $D \subseteq V$ s.t. the application constraints $\mathcal{C}$ are satisfied
$D \leftarrow \emptyset$
$S \leftarrow$ set such that $S_i = \{ j : V_i \in \mathcal{C}_j$ where $V_i$ is the $i$th vulnerability in $V\}$
$c_{S_i} \leftarrow \Sigma_{A \in Pr_A} Pr_A\ (A)\, |\, ExF(A) \cap \{V_i\}\, |$
$\mathcal{C}' \leftarrow [\, |\mathcal{C}|\, ]$
while $\mathcal{C}' \neq \emptyset$ do
$c_{S_i} \leftarrow argmax_{s_i \in s} \frac{|s_i \cap c'|}{s_i}$
    $\mathcal{C}' \leftarrow C' \backslash S_i$
    $D \leftarrow D \cup \{V_i\}$
end while
return $A$
```

6. EVALUATION AND DISCUSSION

Darknet Market Data. We scraped and parsed eight marketplaces located on the Tor network during the month of May 2015. We use a sample of the products in our database to evaluate this game theoretic framework. This is because the exploit function, which associates Darknet exploits with their targeted vulnerabilities was manually specified by the analyst. The product list used for these experiments was comprised of 167 distinct hacking tools. We found several identical products sold on more than one market usually by the same seller (using an identical online handle). The products targeted 21 specific platforms, such as different versions of Adobe Flash, Linux, MS Windows and OS X as well as online presences such as Facebook, WordPress and others. Hardware-related software such as those associated with point-of-sale machines, routers, and servers are also reflected in this number. Figure 6.1 illustrates the variety of products in the markets and Table 6.2 illustrates exemplar exploits in this dataset.

System Configurations. Figure 6.1 illustrates a variety of platforms represented in our Darknet market data. In this paper, we describe results when using application constraints based on common configurations for Windows and Linux servers—as these were the most prominent targets of exploits found on the Darknet. In our experiments, we mapped software such as media players, databases, and FTP server software to application constraint sets to model the functional requirements of a system. We have also created (and conducted experiments with) models for Android, Point-of-Sale, and Apple systems—though qualitatively the results differed little from the Windows and Linux Server experiments.

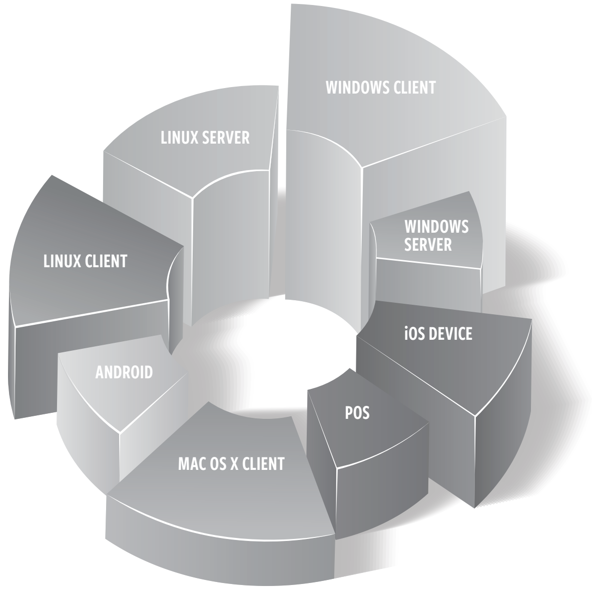


Figure 6.1: Distribution of Exploits with respect to platform.

Product	Vulnerability	Target	USD
Kernel Panic	X-display system	Linux <= 3.13.0-48	$471.56
IE <= 11	memory corr.	IE on Windows <= 7	$35.00
RemoteShell	wpconfig.php	Wordpress MU	$1,500.00
0day RCE	WebView memory corr.	Android 4.1, 4.2	$36.50
WindowsLPE	win32k elev. of priv.	Windows <= 8.1	$12.48
MS15-034 RCE	http.sys	Windows <= 8.1	$311.97
FUD Flash Exp.	unspec.	FlashPlayer <=16.0.0.287	$600.00

Table 6.2: Examples of Exploits from Darknet Markets

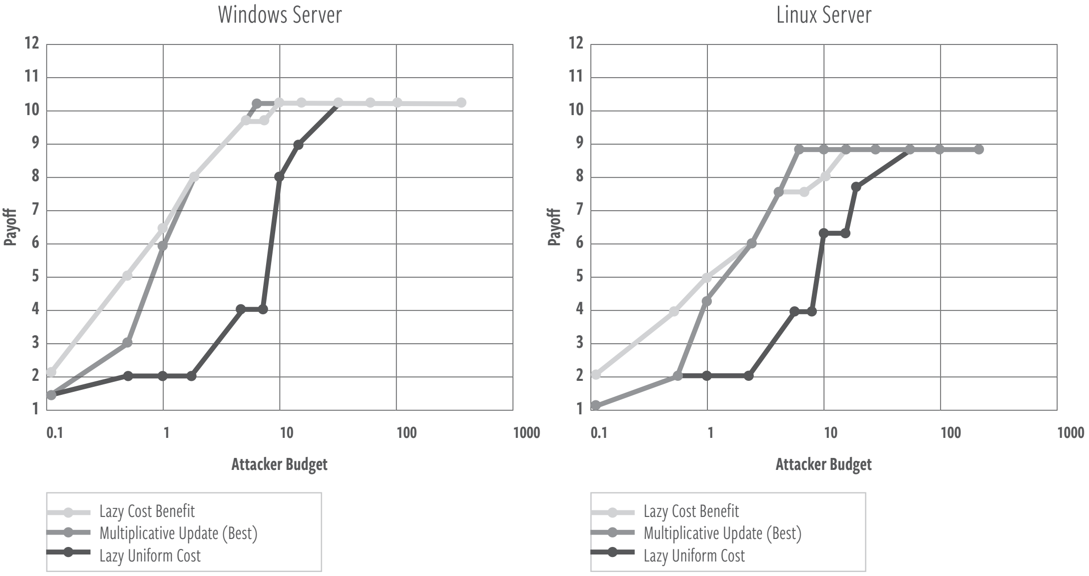


Figure 6.3: DHAP Payoff vs Budget

DHAP Results. We implemented both the greedy and multiplicative update approaches to the DHAP problem. For the greedy algorithm, we studied three variants of greedy (cost-benefit, uniform cost, and combination of the two) while we varied the parameter ϵ for the multiplicative update approach. We examined attacker payoff as a function of budget (in Bitcoin). Figure 6.3 displays this result. Though the cost-benefit greedy algorithm has the potential to perform poorly, it was, in general, the best performing approach—despite the multiplicative update approach achieving the better approximation guarantee. Further, the multiplicative update algorithm (Algorithm 2) was consistently the slowest in terms of runtime, taking much longer than the lazy greedy algorithms, particularly for high values of k_{atk}. Despite the multiplicative update algorithm having a better theoretical approximation ratio when compared to the tandem of greedy algorithms, namely $(1-\epsilon)(1-\frac{1}{e})$ compared to $\frac{1}{2}(1-\frac{1}{e})$, we see in Figure 6.3 that the greedy algorithms performed as well as or better than the multiplicative update very consistently. In all algorithms, as expected, runtime grew with budget (not pictured)—though the relationship was not strict, as an increase in budget does not necessarily mean that more exploits will be selected. In our experiments (on a commodity computer equipped with a 3.49 GHz i7 CPU and 16 GB of memory), our runtimes never exceeded ten minutes.

DHDP Results. Figure 6.4 demonstrate a defender's best response to an attack strategy (generated by DHAP) against a Windows Server and Linux Server, respectively, for varying values of k_{atk}. Though we see similar trends in Figure 6.4 as we do in Figure 6.3, we see that the payoff is generally lower, meaning that the defender can lower the expected payoff by enacting a best response strategy to an attack strategy produced by DHAP—which in our framework translates to fewer exploited vulnerabilities.

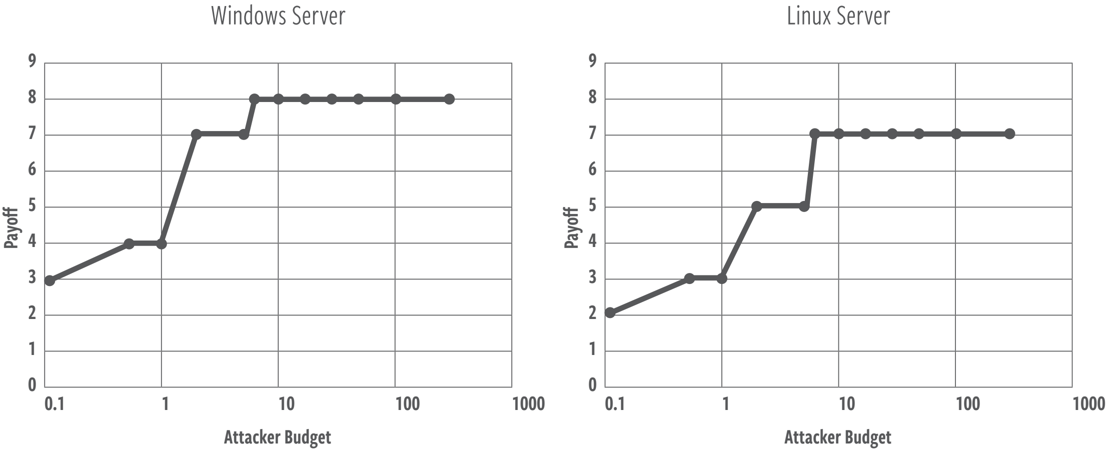


Figure 6.4: Defender Best Response, Payoff vs k_{atk}

Exploit Payoff Analysis. Instead of altering the software that appears on the host system to avoid exploits, such as in the best response approach, in exploit payoff analysis, the defender will identify which specific exploits are increasing the payoff the most. The hope being that the defender can reverse-engineer the exploit, or patch the vulnerability himself. To identify which exploits should be reverse-engineered, the defender first runs DHAP against his host system to identify what payoff an attacker could expect to produce. Then, for each exploit ex, the defender reruns DHAP against the host with the set of exploits $Ex \backslash \{ex\}$. The exploit ex that, when removed from the universe of exploits Ex, produces the largest drop in payoff for the attacker is the exploit that the defender should attempt to reverse-engineer. More formally, let A be the attack strategy produced by DHAP when using Ex as the universe of exploits and let A_{ex} be the attack strategy that is produced when DHAP is run against the host when using $Ex \backslash \{ex\}$ as the universe of exploits. The defender will attempt to reverse-engineer the exploit $ex = argmax_{ex \in Ex}\, p\,(A, D) - p\,(A_{ex}, D)$, where D is the defense strategy representing the host. To account for exploits that, though they greatly reduce payoff when removed from Ex, may be too expensive for the defender to purchase, we also consider a cost-benefit analysis, where the decrease in payoff is normalized by the cost of the exploit (i.e. $ex = argmax_{ex \in Ex} \frac{p(A,D) - p(A_{ex},D)}{C_{ex}}$).* The top exploits to reverse-engineer to defend a Windows Server host when considering an attacker budget of $k_{atk} = 5$, are shown in Table 6.5 with columns for both maximum payoff reduction and maximum cost-benefit analysis.

Exploit	Payoff Reduction	Max Cost-Benefit	Exploit Cost (BTC)
SMTP Mail Cracker	1	4.757	0.2102
SUPEE-5433	1	1.190	0.8404
Hack ICQ	1	79.089	0.01264
Plasma	0.6677	1.582	0.2563
WordPress Exploiter	0.6677	2.6467	0.2102
CVE-2014-0160	0.6677	3.178	0.2101

Table 6.5: Defender Exploit Analysis for $k_{atk} = 5$

* (i.e. $ex = argmax_{ex \in Ex} \frac{p(A,D) - p(A_{ex},D)}{C_{ex}}$)

7. CONCLUSION AND FUTURE WORK

We detailed a data collection system for gathering information from Darknet exploit markets and hacker forums. Additionally, we defined a game theoretic framework with which we can analyze the Darknet data, providing system-specific policy recommendations to system administrators. For the framework, we formalized decision problems for both the attacker and the defender, subsequently proving complexity results and providing approximation algorithms for each problem. We also evaluated the framework on a real-world dataset gathered from the previously discussed exploit markets.

In future work, we plan to extend the game-theoretic framework to include non-deterministic problem formulations, and construct algorithms to generate mixed strategies for the attacker and defender. By extending the exploit function in the framework, we plan to support blended threats, where the number of vulnerabilities affected by a cyber-attack is a superset of the union of the vulnerabilities affected by each individual exploit (i.e. $ExF(A) \supseteq \bigcup_{a \in A} ExF(\{a\})$). Additionally, we want to closely integrate the game theory framework with the crawling and parser infrastructure to provide system policy recommendations based on real-time data. We are continually adding support for additional Darknet sites in our scraping pipeline to gain a better understanding of the cyber threat landscape.

ACKNOWLEDGEMENTS

Some of the authors of this work were supported by the U.S. Navy, Office of Naval Research, NEPTUNE program as well as the Arizona State University Global Security Initiative (GSI), and the ASU Institute for Social Science Research (ISSR). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research. We thank Anum Naveed, of IntelliSpyre, Inc. for his feedback on this paper.

REFERENCES

L. Ablon, M. C. Libicki, and A. A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Rand Corporation, 2014.

Y. Azar and I. Gamzu. Efficient submodular function maximization under linear packing constraints. *ICALP,* 1:38–50, 2012.

S. Chakrabarti, M. Van den Berg, and B. Dom. Focused crawling: a new approach to topic-specific web resource discovery. *Computer Networks,* 31(11):1623–1640, 1999.

H. Chen. 2011. Dark web: Exploring and data mining the dark side of the web. Vol. 30. Springer Science & Business Media.

R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13,* SSYM'04, pages 21–21, 2004.

U. Feige. A threshold of ln n for approximating set cover. *J. ACM,* 45(4):634–652, July 1998.

T. Fu, A. Abbasi, and H. Chen. A focused crawler for dark web forums. *Journal of the American Society for Information Science and Technology,* 61(6):1213–1231, 2010.

M. Jain, Dmytro Korzhyk, Ondˇrej Vanek, Vincent Conitzer, Michal P ˇ echou ˇ cek, and Milind Tambe. 2011. A double oracle algorithm for zero-sum security games on graphs. In The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. International Foundation for Autonomous Agents and Multiagent Systems, 327–334.

D. Lacey and P. M. Salmon. It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. In D. Harris, editor, *Engineering Psychology and Cognitive Ergonomics,* volume 9174 of *Lecture Notes in Computer Science,* pages 117–128. Springer International Publishing, 2015.

J. Leskovec, A. Krause, C. Guestrin, C. Faloutsos, J. VanBriesen, and N. Glance. Cost-effective outbreak detection in networks. In *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining,* pages 420–429. ACM, 2007.

F. Menczer, G. Pant, and P. Srinivasan. Topical web crawlers: Evaluating adaptive algorithms. *ACM Transactions on Internet Technology (TOIT),* 4(4):378–419, 2004.

M. Minoux. Accelerated greedy algorithms for maximizing submodular set functions. In J. Stoer, editor, *Optimization Techniques,* volume *7 of Lecture Notes in Control and Information Sciences,* pages 234–243. Springer Berlin Heidelberg, 1978.

G. Nemhauser, L. Wolsey, and M. Fisher. An analysis of approximations for maximizing submodular set functions. *Mathematical Programming,* 14(1):265–294, 1978.

E. Nunes et al., Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence. IEEE Conference on Intelligence and Security Informatics (ISI-16), 2016.

J. Robertson, V. Paliath, J. Shakarian, A. Thart, and P. Shakarian. Data driven game theoretic cyber threat mitigation: Twenty-eighth aaai conference on innovative applications of artificial intelligence, 2016.

P. Shakarian and J. Shakarian. Considerations for the development of threat prediction in the cyber domain.*AAAI Workshop on Artificial Intelligence for Cyber Security (AICS),* 2016.

P. Shakarian, J. Shakarian, and A. Ruef. *Introduction to cyber-warfare: A multidisciplinary approach.* Elsevier, 2013.

K. Soska, and N. Christin. "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem." *24th USENIX Security Symposium (USENIX Security 15).* 2015.

Milind Tambe. 2011. Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned (1st ed.). Cambridge University Press, New York, NY, USA.

Wei, Wang. "Hunting Russian Malware Author Behind Phoenix Exploit Kit". The Hacker News. 2013. http://thehackernews.com/2013/04/hunting-russian-malware-author-behind.html

Ziming Zhao, Gail-Joon Ahn, Hongxin Hu, and Deepinder Mahi. 2012. SocialImpact: Systematic Analysis of Underground Social Dynamics. In ESORICS (Lecture Notes in Computer Science), Sara Foresti, Moti Yung, and Fabio Martinelli (Eds.), Vol. 7459. Springer, 877–894. http://dblp.uni-trier.de/db/conf/esorics/esorics2012.html#ZhaoAHM12

NOTES

1. Corresponding author: shak@asu.edu.
2. See the Tor Project's official website (https://www.torproject.org/).
3. https://www.fireeye.com/blog/threat-research/2015/06/evolution of _dridex.
4. http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-americancybercrime-n22371.

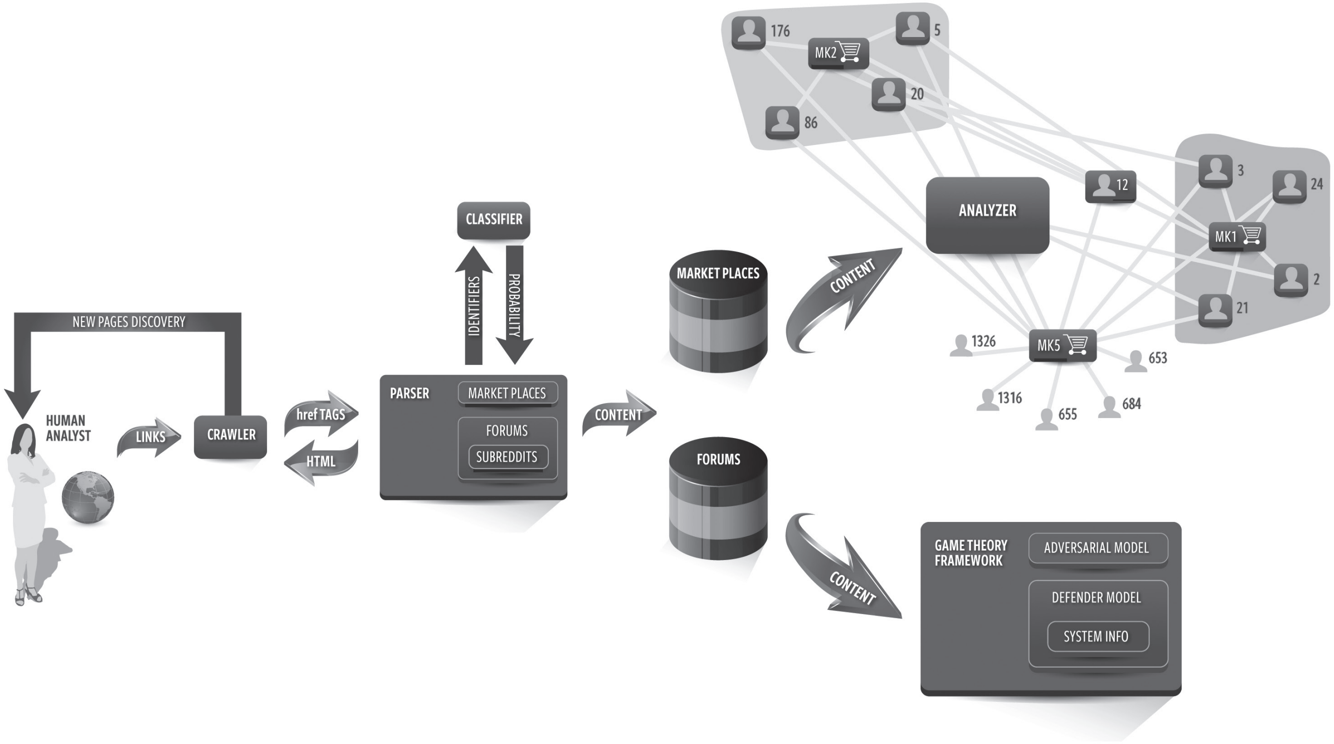


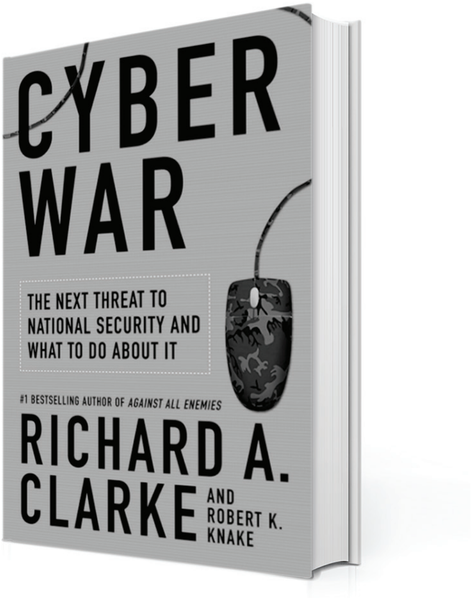
Figure 4.5: System Overview (Enlarged to show detail.)

The Cyber Defense Review

◈ Book Review ◈

Cyber War
by Richard A. Clarke and Robert K. Knake

Reviewed by Professor Chris Arney and Second Lieutenant Joseph Kozlak


CYBER WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE AND ROBERT K. KNAKE

This book takes a holistic view of the cyber world and how it pertains to the United States regarding capabilities, vulnerabilities, policy, and potential strategies. We, as student and instructor in a course entitled *Networks for Cyber Operations* used this book as one of our texts in the Spring semester of 2016. Author Richard Clarke uses his experience in dealing with nuclear weapons, and his role as a Special Advisor to the President for Cyber Security to explain how the world situation has changed to make cyberattacks a significant threat to the United States. Clarke and Knake do an excellent job of speaking to a general audience (from cyber novices to experienced cyber warriors and hackers). The authors introduce the subject by describing the Israeli cyberattack on Syria before the bombing of a nuclear facility in 2007. This book stays away from the technical aspects of cyberattacks, but provides detailed background information about the Internet and how digitization has created a new battlefield.

Chapter 1, *Trial Runs* dives into how cyber disturbances in network capabilities such as crashing specific websites can be a precursor to the use of kinetic force. This chapter sets the background for how cyber war has been conducted in the past and illustrates some potential vulnerabilities for future attacks. The authors suggest there is a “credible possibility that such conflict may have the potential to change the world military balance and thereby fundamentally alter political and economic relations.” (p. 53) This is the nature of conflict now, instead of a precision-guided munition targeting a specific area, a cyberattack can cripple an entire nation. Clarke describes in Chapter 2 how cyber units and systems are structured in the United States, Russia, and China. This sets the tone for his future discussion on the United States' cyber policy of the future. Chapter 3, *Battle Space* was our favorite as it detailed the variety of different elements that hackers' target. Clarke's explanation of the Trojan horse in a historical context was helpful in seeinghow vulnerabilities are exploited in the cyber world. It is easy for a code writer to add a couple of lines of code to software that can act as a logic bomb or the Trojan horse in the Internet. Furthermore, as society, especially commercial businesses, become more and more dependent on the Internet, there is a greater probability of someone becoming a victim of a catastrophic cyberattack. The need for cyber defense has grown with digitization, but how to build that defense is the vexing question of today.

Resilient defense of our networks is nearly impossible, and the ability to reliably and effectively retaliate is problematic because of the attribution challenge. Clarke uses the metaphor of an art thief and a hacker: "The difference between art thieves and world-class hackers is that with the best of the cyber thieves, you never know you were a victim." (p. 162) This is the issue that makes cyber defense so difficult, we do not know how or what a hacker is going to target, and when they do attack, we do not necessarily have alarms that sound. The hackers may leave with mountains of information yet not knowing if they stole any of it because we also have possession. If we cannot protect everything, we must protect our most valuable networks. But how we do that is still the question. The authors write with candor and strong opinions making the subject come to life for the reader.

After Clarke and Knake provide the background of attacks, hackers, and the vulnerabilities in cyberspace, they dive into explaining the creation of policies to deal with cyber operations. Clarke discusses the creation of a Defensive Triad. His background in Cold War politics dealing with nuclear weapons factors into this triad proposal. Cyber is different than the nuclear weapons of Cold War deterrence because cyber deterrence does not happen the same way. For one thing, if you do not use your cyber weapons periodically, no one will know or think you have the capabilities. Clarke discusses a practical illustration of cyber war, which is useful for readers interested in the future possibilities of cyber warfare. This chapter takes a step-by-step approach to explaining the different aspects and consequences of cyber war with a nation like China. Powerful nations have not gone to war with each other since World War II because of the deterrence of the lethal capabilities that such nations' possess, but now war can take place on the new cyberspace battlefield in which soldiers are not in direct combat. Finally, Clarke proposes his agenda to secure our systems and deter other nation states from attacking our networks.

Cyber War is a non-technical read that gives valuable insight into past, current, and future cyber situations and capabilities. The strength of this book is that it offers something meaningful for every reader. Clarke's stories add to the book's excitement by applying context to his theories of cyber operations. He adds valuable insight because of his background. This book is a call for action because the US government has been so focused on the wars in Iraq and Afghanistan that nations such as Russian and China may have moved ahead of the United States in the cyber domain. This is an excellent book for anyone looking to learn more about cyber capabilities and cyber policies in the United States.

Cyber War

Author: Richard A. Clarke and Robert K. Knake
Publisher: Harper Collins e-books, 2010
e-book: 351 pages
Language: English
ISBN: 978-0-061-99239-1

Chris Arney is a Professor of Mathematics at the United States Military Academy and former Head of the Department of Mathematical Sciences. He holds a Ph.D. in Mathematics and M.S. Degrees in Computer Science and Mathematics from Rensselaer Polytechnic Institute. He also holds a B.S. from the United States Military Academy. A career Military Intelligence officer, he served in tactical assignments, teaching assignments at USMA, and research positions at NASA Langley Research Center and the Army Research Office. His current research includes cooperative game theory, applications of network science, and mathematical applications to cyberspace.

Second Lieutenant Joseph Kozlak is currently assigned to 2-11 Infantry Regiment at Fort Benning, GA for Infantry Basic Officer Leadership Course. His follow on assignment is 3rd Brigade, 2nd Infantry Division at Fort Lewis, WA. Prior to commissioning in 2016, he received a B.S. with honors in Mathematical Sciences from the United States Military Academy. He was a four-year letter winner and two-year captain in hockey at USMA.

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

SUBMISSIONS FOR CDR ONLINE

The Cyber Defense Review Online (CDR) 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 1 • NUMBER 2

FALL 2016

THE CYBER DEFENSE REVIEW

Attacking Cyber: Increasing Resilience and Protecting Mission Essential Capabilities in Cyberspace
Lieutenant General Larry Wyche
Dr. Dawn Dunkerley Goss

Special Operations Forces Truths – Cyber Truths
Major General Stephen G. Fogarty
Major Jamie O. Nasi

Four Imperatives for Cybersecurity Success in the Digital Age: We Must Flip the Scales — *Maj. Gen. John Davis, USA, Ret*

Preparing for a Bad Day – The importance of public-private partnerships in keeping our institutions safe and secure — *Mr. Thomas J. Harrington*

Cyber Education via Mathematical Education — *Professor Chris Arney*, *Major Natalie Vanatta*, *Major Thomas Nelson*

Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex — *Dr. Mark Raymond*

INTRODUCTION
Discussions from the Front Lines of the Cyber Domain — *Colonel Andrew O. Hall*

BOOK REVIEW
Cyber War by Richard A. Clarke and Robert K. Knake — *Professor Chris Arney*, *Second Lieutenant Joseph Kozlak*

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 PDFs).
- ✓ 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.