VOLUME 4 ◆ NUMBER 1 SPRING 2019

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
Spellman Hall
2101 New South Post Road
West Point, New York 10996

SUBMISSIONS
The Cyber Defense Review
welcomes submissions at
mc04.manuscriptcentral.com/cyberdr

WEBSITE
cyberdefensereview.army.mil

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

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters. The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

RESEARCH ARTICLES

RESEARCH NOTE

BOOK REVIEW

The Cyber Defense Review

Introduction

VOLUME 4 • NUMBER 1

The Cyber Defense Review: The Importance of Partnerships in the Cyber Domain

Colonel Andrew O. Hall

INTRODUCTION

Welcome to another provocative edition of the CDR, which explores the importance of partnerships in the cyber environment. Crucial to the success and growth of the Army Cyber Institute (ACI) is the development of impactful partnerships. We are most proud of our special relationship and partnership with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. The NATO CCDCOE is a global thought leader in the discussion and advancement of critical cyber issues—technology, strategy, operations, and law. Each year NATO CCDCOE hosts their prestigious International Conference on Cyber Conflict (CyCon) in Tallinn. This year's CyCon conference theme of "Silent Battle" seeks to foster a conversation on topics such as vulnerabilities, exploitations and patches, threat detection and attribution, and situational awareness to wage this 'silent battle.' The ACI will support this magnificent event with speakers, West Point cadet participation, and distribution of the Spring CDR to all attendees. We at the ACI believe that operational success in the cyber domain derives from the development and evolution of strategic partnerships. We are excited that the CDR facilitates impactful partnerships and is at the fulcrum of the global cyber conversation.

I am continually impressed with the quality of our CDR contributors as they push the envelope regarding the scope of their research and analysis. Our Spring issue opens with an article from Rear Adm. Danelle Barrett and Mr. Andrew Mansfield that addresses the reality and potential of cloud computing in the Navy and DoD. The ACI is experimenting with the renewed tactical applications of HF communications, partnering with conventional and SOF units during their rotations at the U.S. Army National Training Center and Joint Readiness Training Center. An outgrowth of this critical work is the collaborative article from BG Robert L. Edmonson, BG David Doyle, LTC Ryan Seagreaves, and MAJ Matthew Sherburne that unmask some of the tactical employment considerations and misconceptions of HF communications. Our Leadership Perspective section concludes with an exciting article from

Colonel Andrew O. Hall is the Director of the Army Cyber Institute where he directs and oversees research, leader development and partnership efforts in the cyber domain. 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 in infantry and artillery units and on the Army Staff and the Joint Staff.

MG (Ret) George Franz, LTC Galen Kane, and LTC Jeff Fair that focuses on the reshaping of cyber intelligence operations to combat new challenges and find opportunities for success on the silent battlefield. We also feature a multi-dimensional Professional Commentary from returning CDR author Oz Sultan, Chief Strategist at Sultan Interactive Group, where he examines disinformation and the growing danger of online terrorism.

Diving into the deep end of our Research section, the CDR features four well-crafted and articulated works that provide our readership with a fresh perspective on cyber partnerships. LTC Christopher Heatherly and Cadet Ian Melendez (Army ROTC at Washington State University) argue that through a new and improved cyber education program, the U.S. Army could expand its cyber reach to all Soldiers. In the next research article, Dr. Robert R. Hoffman introduces readers to the concept of a 'Campaign of Experimentation' for cyber operations. This thought-provoking piece explores new concepts to enhance offensive and defensive cyber operations. MAJ Michael Klipstein from the ACI guides readers in an understanding of the quantification and visualization of offensive cyber operations risk. This research effort asserts that a quantifiable framework could mitigate the lack of national-level expertise for offensive cyber operations. The research section concludes with an engaging article from Dr. Milton Mueller, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei as they delve into the legal aspects of institutionalizing a transnational cyber attribution policy.

We continue our tradition of providing high-impact Research Notes to our readers with an article from COL Stoney Trent, Dr. Robert R. Hoffman, LTC David Merritt, and CPT Sarah Smith, as they model the cognitive work of cyber protection teams. To complete this edition of the CDR, we are thrilled to introduce you to the ACI's staff lawyer, Courtney Gordon-Tennant. In Courtney's review of *Code Girls: The Untold Story of the American Women Code Breakers of World War II*, by Liza Mundy, we learn about the tremendous accomplishments of American female codebreakers during the early days of cyber.

As we discussed in the Fall issue, the CDR and ACI are continuing the cyber conversation with the establishment of the CDR Press. Our inaugural CDR Press publication is entitled *Nonsimplicity, The Warrior's Way* by Dr. Bruce West and Dr. Chris Arney. This important work explores complexity science and suggests appropriate changes in policies, procedures, and principles are needed in the U.S. military; specifically, addressing the implications to the individual as these changes are made.

In becoming the journal of choice for cyber practitioners and to further push the conversation, we are excited to announce the introduction of a SIPR-based CDR. This will be a space where rich cyber conversation can take place in a meaningful and impactful manner. With this new avenue for discussion, we are seeking SIPR accessible researchers to submit articles, blogs, white papers, briefings, and research notes. Our featured blogs will allow the conversation to continue informally and in a free-flowing manner. These new projects will allow cyber practitioners the opportunity to publish innovative and thought-provoking works. As always, these two endeavors are in keeping with the ACI and CDR's tradition of advancing the body of knowledge. There will be further updates to come regarding the SIPR CDR, but for now, as General Douglas MacArthur once said, "keep your ear to the ground."

Along with the establishment of the CDR Press and the new SIPR CDR, we are partnering with the Palo Alto Networks' Cybersecurity Canon to establish new standards and format for our CDR book reviews. The Cybersecurity Canon has a laser-focus on education and highlights must-read books for all cybersecurity practitioners. This well-thought-out book review format can be viewed at https://cybercanon.paloaltonetworks.com and will ensure the quality of reviews is consistent across the CDR's cyber conversation.

Our theme of partnerships extends to the CDR Editorial Board. This world-class group of scholars exemplifies the importance of partnerships as they collectively transform the CDR. At our inaugural Board meeting at the CyCon U.S. Conference in Washington DC last November, members provided recommendations to improve quality and reach, which will increase CDR standing and product. Our members agreed the CDR's 'sweet-spot' regarding content is to tackle the Big Issues. We had a lively discussion among all Board members regarding the potential benefit of themed or area issues with suggested topics: 1. Information Warfare, 2. Law & Policy, 3. Military Leadership in the Cyber Domain, and 4. Cyber Conflict. Board members suggested the CDR participate in major cyber conferences to increase exposure and endorsed greater international focus for CDR articles and authors. The CDR was encouraged to develop global partnerships with cyber stakeholders. All Board members volunteered to act as Ambassadors for the CDR and assist with attracting new authors. I look forward to our second meeting, which will be held in September, here, at the United States Military Academy at West Point.

I want to thank Michelle Marie Wallace, Sergio Analco, Gina Daschbach, SGM Jeff Morris, Courtney Gordon-Tennant, and Tony Rosa for their exceptional contributions to this edition. Their talent, creativity, and tireless effort are instrumental in the CDR's success. As always, we are excited to continue the cyber conversation together.

The Cyber Defense Review

Senior Leader Perspective

The Challenge and Opportunities of Standing on Cloud – Finding our Warfighting Advantage

Rear Admiral Danelle Barrett
Andrew Mansfield

The Navy is dealing with the challenges of a world where exponentially accelerating and converging technologies impact the way we operate at unprecedented speeds. We must quickly leverage the operational advantages emerging technologies bring to warfighting and be forward-leaning in disrupting their use by adversaries. Similarly to how cloud technologies and Smartphones have fundamentally changed the way we live by accessing and using information in revolutionary ways, victory in warfighting will go to those forces with similar information supremacy. Cloud technologies provide an opportunity to achieve that supremacy, enabling extraordinary benefits through scalable services which support Big Data analytics, Artificial Intelligence (AI), and machine learning. Transition away from stove-piped capabilities and sources of data to a cloud environment where authoritative data can be exposed, discovered, and shared for improved situational awareness and decision making is the future. However, the move to the cloud does not come without risks and challenges.

Naval operators must understand the risk of data in the cloud and ensure appropriate oversight of our information in the new cloud environment. Provisioning cloud to the tactical edge also poses challenges: synchronizing data between ashore and afloat, and moving information in the most efficient, secure, and operationally relevant manner. Finally, while cloud technology presents opportunities, the most significant challenges will be human. Cultural barriers to sharing information and training the Navy force to think about information in a new way must be addressed. Humans and machines will combine to define the context of data to become self-aware, self-learning and act predictively, doing the heavy lifting to correlate and use information at a speed and level of complexity our brains are incapable of today. There are no bystanders in this effort. It will take all hands in active engagement to understand the tools at our disposal and use them to achieve unparalleled warfighting effects.

Rear Adm. Danelle Barrett graduated from Boston University in 1989 with a Bachelor of Arts in History. She holds Master of Arts degrees in Management, National Security/Strategic Studies, Human Resources Development and a Master of Science in Information Management.

Her operational assignments include tours at U.S. Naval Forces Central Command/U.S. 5th Fleet; 2nd Fleet, Carrier Strike Group 2, Multi-National Forces Iraq, Carrier Strike Group 12, with deployments supporting Operations Enduring Freedom in Afghanistan and Unified Response in Haiti; and deputy director of current operations at U.S. Cyber Command. Her multiple shore tours include commanding officer, Naval Computer and Telecommunications Area Master Station Atlantic; and chief of staff, Navy Information Forces Command.

Barrett currently serves as the Director of Navy Cyber Security.

Personal awards include Copernicus Awards 1998, 2000 and 2005; DoD Chief Information Officer Award, first place individual category 2006; Federal 100 2010; AFCEA Women in Leadership Award 2014; Women in Technology Leadership Award 2017. She has published 29 articles.

To understand how to use the cloud for operational warfighting lethality and improved efficiencies, it is important to understand what the cloud is. "Cloud" is the current buzzword of the day in strategy and marketing briefs, but it is hardly a catchphrase in practice. It is Information Technology (IT) delivered as a service to enable access to information from anywhere, at any time, and is not limited to specific machines or systems. Unlike traditional client/server architectures, it provides a platform to rapidly configure and expand resources and capabilities and enables orders of greater magnitude, speed, and agility to deploy and integrate that capability. Cloud facilitates improved cybersecurity of information through precise monitoring of access points to protect information from unauthorized use. The commercial industry has invested heavily in cloud research and development, and those technologies and services matured at unparalleled rates, a trend that is expected to accelerate. This can contribute to the confusion about what the cloud is. As cloud momentum in the commercial industry continues at breakneck speed, even the term cloud will morph as the next business and technical architecture replaces the cloud of today. The Navy needs to stay aligned with industry best practices and employment of the latest models so that we seamlessly transition and evolve our IT on pace with industry.

To understand cloud as a warfighting enabler, it's important to note cloud is not simply "someone else's computer." The reality is much more expansive as cloud design and capabilities cover the breadth of IT, from networks, hardware, computer management capabilities, and storage of data, software platforms, and the applications that ride upon them. Cloud is a way of looking at IT as a set of discrete, distributed, and malleable services and capabilities. Those capabilities are not tied to any specific piece of hardware, software or network. Industry has led an adherence

Andrew Mansfield is the Naval Information Warfare Center (NIWC), Atlantic Executive for Network Centric Development and Integration. He serves as the Technical Director of NIWC. He engages at a national level in charting the course for the Navy's IT modernization efforts, specializing in areas of commercial cloud/cloud transformation, Data Sciences and Analytics, and Cyber Security. Mr. Mansfield was appointed as an SL in October 2011 and has over 33 years of federal service. His contributions include: Serving as the 5.0 Engineering Lead/ Chief Engineer and as the national lead for Net-Centric System-of-Systems Engineering and Integration (SE&I). He led the modernization of the Veteran's Administration Chapter 33 GI Bill Benefits capability and was the National and Local Lead for the Command & Control (C2) and Business Information Technology (IT) Competency.

to open standards and cloud technologies have matured to a point where they are interoperable, widely available, and easily consumable.

Cloud means Navy content owners and application developers can now design, engineer, integrate, and continuously evolve each of these architectural elements in the cloud almost entirely independently from each other while still retaining overall integration and interoperability. It also makes the infrastructure agile and flexible enough to holistically adapt and scale up and down to the available capacity (i.e. network, processing, and data storage needs).

Cloud can be used to develop and execute offensive operations to deny adversaries access to their information at the time of our choosing. On a ship at sea or a tent in the desert, warfighters will manage the local hardware and software to access the cloud at the tactical edge, synchronized with a larger cloud ashore, allowing operators to be self-sustaining in a fight. Extending key portions of Navy cloud infrastructure to the tip of the spear will enable the Navy to employ the higher-level AI and machine learning to expedite command and control, operations, and improved decision making at the tactical edge. Cloud is necessary to enable next-generation technical capabilities such as Internet-of-Things (IoT), AI, Human-Machine Teaming, and Augmented Reality. By combining cloud computing with new warfighting Tactics, Techniques, and Procedures (TTPs), operators will have decision advantages and the ability to generate operational effects at the tactical edge not achievable with legacy IT infrastructure. This includes providing a platform for executing tactical cyber offensive and defensive effects. On the defensive cyber side, the flexibility of cloud technologies enables our ability to maneuver around adversaries' defenses while strengthening our defenses by minimizing disruptions.

From a cyber operations perspective, the unique capabilities of cloud computing can be applied in several ways. In the thick of battle, the warfighters can be limited by the information available, particularly with our dependence on satellites to reach back to shore. It is critical to have an end-to-end information platform that synchronizes our ashore and afloat cloud environments and to exchange data specific to that ship Commander's mission. Unlike current architectures where capabilities are typically tightly coupled to the hardware they're delivered with, cloud can maximize IT to its fullest extent. The ability to surge computational resources for high priority operational missions, including cyber offensive operations, could be prioritized and allocated quickly through automatic scaling by design. Cyber tool capabilities will be helped by computing capacity in a cloud environment and given priority access to infrastructure resources needed to execute operations. Cloud analytics have the potential to identify adversary network vulnerabilities at greater speed and precision, while simultaneously protecting our resources, making systems more resilient for fighting through attacks.

This rapid means of discovery and situational awareness of the adversary using cloud provides speed to effects. Cloud-enabled AI will aid cyber operators to see the cyber battlespace in near real-time, constructing and modeling ad-hoc capabilities for tactical warfighters to employ. For example, a team of Marines that is preparing to breach a building, having deployed from a littoral amphibious combat ship, could benefit from cloud-enabled AI. The building itself has security measures, locks, cameras, lights, etc. Unmanned platforms, working in conjunction with cyber tools and sensors are deployed. They quickly scan networks to build an initial view of the security systems and infrastructure in the building. This data is relayed back to the littoral platform and loaded into the tactical cloud for quick forensic analysis. Working in the tactical cloud and reaching back to greater cloud resources ashore when available, offensive cyber operators can create custom measures informed by the latest intelligence, test their assumptions on the tactical edge cloud, then load the cyber counterattack strike package on the deployed systems. Using the near real-time intelligence, the ground forces near the building receive constant updates and have accurate situational awareness of the environment to move with confidence around the battlespace. They know what devices are connected in the building and may even have sensors to provide visibility on combatants located inside. Should the adversary launch weapons to deny access to the cloud or strike platforms, advanced cloud network sensors could rapidly detect this activity and adapt by pre-emptively reconfiguring pre-approved counterattack strike packages and system defensive counter-measures to continue the attack. Data from the attack are used for trend analysis of adversary TTPs, building a repository of shared knowledge between all ships and back through the shore cloud to the Department of Defense (DoD) and other partners. While this sounds like science fiction, it is possible with today's technology, and cloud provides the needed capabilities to make it happen. Using the cloud for collaboration, AI, Big Data analytics, and to rapidly reconfigure resources to act and provide digital representation of an enemy system, gives cyber warriors at the tactical edge the platform they need to execute cyber operational effects.

Getting the cloud as a platform to the tactical edge to achieve this kind of warfighting advantage requires us to innovate how we provide our IT infrastructure afloat. In buying commercial cloud as a service from end-to-end, from the enterprise ashore to the tactical edge afloat, we must challenge all existing models in use for developing and delivering information capabilities. Under the Navy's "Compile to Combat in 24 Hours" initiative to transform the information environment across the enterprise, options are being explored for permanent commercial cloud services and infrastructure extended shipboard to replace government-owned infrastructure for processing, accessing, and displaying information. In this cloud infrastructure, shared servers, used by many application owners to host software code and data, would remain owned and maintained by the commercial vendor.

The Consolidated Afloat Network Enterprise Services (CANES) is the program that modernizes shipboard network hardware and software, and the shared computing environment described above represents "the brains" of CANES networks afloat in the government model. By modularizing the "brains" from the rest of the CANES infrastructure (routers, switches, workstations, etc.), the commercial vendor could modernize software elements instantaneously and update hardware more frequently to improve information processing. The vendor's tools, analytics, and improved cybersecurity capabilities would be purchased as part of the service, improving reliability and efficacy of information to support operations. They could also ensure synchronization of the afloat and ashore data clouds and enhance the quality of service by tagging and compressing data to move in a prioritized manner. This would get us to a level of information superiority that is not achievable with today's infrastructure, allowing operational commanders to get the right information at the right time.

All the benefits of using commercial vendors to provide cloud services come with risks and we must be deliberate in how we protect our information in the cloud. Even in that, however, there are advantages to cloud. Today, the Navy has myriad combinations of network hardware and software across the Navy enterprise that lack rigorous configuration management and pose an increased surface for cyberattack. Certainly, significant defense in depth investments were made over the last several years to build in resiliency and reduce our attack surface, but commercial cloud offers us opportunities to further improve this environment. Storing Navy information in the commercial cloud allows us to move at "industry speed" in employment of cybersecurity upgrades and processes, in addition to the other benefits of big data use outside the cybersecurity arena. Industry does not, however, have a long track record of decades of commercial cloud provisioning and it is prudent to fully understand how information will be protected in this new shared cloud responsibility model. The movement of Navy information to the commercial cloud must be executed in a deliberate manner with an understanding and acceptance of this risk and in comparison with the risk of continuing along the current path with its own significant cybersecurity challenges. Note that this is true in all our security domains. There will be separate cloud environment offerings for classified and unclassified information, provided by government and commercial industry.

Over the past year, the Navy has been working closely to define an initial model for "Command and Control" (C2) of Navy information in the commercial cloud. Specific actions must be performed to ensure C2 of our information in that environment that may be unique to how the Navy or DoD operates. For example, during a cybersecurity incident, a commercial vendor may be required to start an incident response. However, doing this may cause a loss of cyber activity situational awareness needed for other purposes. This requires collaboration with vendors, cybersecurity operators, and engineers to develop a detailed shared responsibility model, where cybersecurity tasks, data, and reporting requirements are well coordinated and implemented between government and industry. We are also ensuring we have standardized contracting language to enforce the requirements with our partners. Navy contracting language needs to provide for a decision window to approve moving forward for incident response or waiting while Navy cyber operators hunt an adversary. Acquisition professionals will ensure contracts are properly standardized for C2. Cyber operators and information owners can have the confidence to access the information when and where needed, and that lines of responsibility and accountability are well defined. As more partners enter the field, the model will continue to evolve.

This same model is needed across the DoD and so the Navy has shared this C2 construct with DoD teams working cloud contracts. Additionally, as the DoD and the Navy continue to harden their networks, adversaries increasingly look to softer targets to get at Navy information. There has been a significant increase in intrusions across industry to include Cleared Defense Contractors (CDCs) and their subcontractor networks to steal information. Options should be explored for CDCs and others who handle Navy information to store that in Navy commercial cloud environments where C2 can be properly executed, and we would have increased confidence in the cybersecurity of their data environment.

Making the cloud-enabled warfighting environment real is not just a technology challenge, it involves people, processes, and technology changes that are fundamentally transformational to how we operate today. We must prepare across all disciplines to embrace the capabilities enabled by cloud, adapting to this new IT ecosystem. Training should be integrated into all areas on how to manage, maintain, and operate on a cloud-driven information warfare platform.

The biggest challenges will not be technological. Fundamental changes in the culture of how we design, field, and deploy IT are needed, and cloud technology allows for an improved model over traditional IT deployment. This change includes networks afloat running AI at the tactical edge cloud to automatically reconfigure based on the operator need and responding and recovering from enemy attacks without a human in the loop. This highlights the increasing trust and confidence in machines' ability to make informed decisions with precision and speed.

Cloud is necessary to move the Navy to the next level of warfighting superiority, addressing challenges posed, particularly by near-peer competitors as defined in the National Defense Strategy. Our information warfare platform needs cloud and its benefits to ensure success across all warfighting lines. As our adversaries can buy the same capabilities, our dominance will depend upon our agility and innovation to quickly deploy cloud to achieve unmatched warfighting effects. As noted by the Chief of Naval Operations and other senior leaders, cyber and space will be where we see the battle beginning—and its end will hinge on the resilience, agility, speed, and flexibility with which we deploy cloud and capabilities which leverage them for our deployed forces.

Tactical Employment Considerations of HF Radios in the Cavalry Squadron

Brigadier General Robert L. Edmonson, II
Brigadier General David S. Doyle
Lieutenant Colonel Ryan D. Seagreaves
Major Matthew G. Sherburne

There are a few misconceptions about the use of High Frequency (HF) communications in the U.S. Army today, especially in a Decisive Action Training Environment (DATE). Based on the US military's experiences in Iraq and Afghanistan with theater provided equipment, leaders assume that HF will provide the means to conduct a one-for-one exchange of a unit's typical slate of FM nets to include Command, O&I, A&L and Fires that are each operated on a separate radio. Others assume that since putting an HF radio into operation is relatively easy, units should be able to put an HF network into operation with ease. The truth is that units only have enough HF radios to establish communications between key leaders. To put them into operation in an effective HF network requires a higher level of training and understanding than units currently have. The network is what is needed for effective Mission Command. This article records the observations of Cavalry Squadron's HF use at the Joint Readiness Training Center (JRTC), illuminate why units struggle, and convey recommendations and resources for HF training at home station so units can maximize their HF capabilities for employment in a DATE scenario and prepare for potential large-scale combat operations.

Observations of Cavalry Squadron HF use at JRTC

JRTC Observer-Coach/Trainers (OC/T's) can summarize a Cavalry Squadron's HF use with just three words: not very much. We use Cavalry Squadrons as an example in this paper because they have the most HF radios on their modification table of organization and equipment (MTOE) compared to other battalions in the Brigade Combat Team (BCT). Frequently, units will report that their HF is 'up' or 'green,' however, in most cases JRTC OC/T's observe that this really means the unit sets up and turns on the HF radio, but they have not made communications checks to any other station.

BG Robert L. Edmonson, II currently serves as the U.S. Army Forces Command, Deputy Chief of Staff, G-6. BG Edmonson began his Army career in 1991 as an Infantry Officer before becoming a Signal Corps Officer. His major assignments include the 101st Airborne Division (AASLT), 82d Airborne Division, Joint Staff Pentagon, Army Staff Pentagon, and Army Intelligence & Security Command.

BG Edmonson last served as the 38th Chief of Signal and Commandant of the Army Signal School where he was responsible for the initial military training and professional military education for nearly 65,000 Signal Corps Soldiers across the Active Duty, National Guard, and Army Reserve Components. He has commanded at every level. BG Edmonson received an Army commission through Frostburg State University, holds a master's degree in Information Resource Management from Central Michigan University, and a master's degree in National Security Strategy from National Defense University, Washington D.C.

What OC/T's commonly observe are two methods of employment. In the first method, they see the reconnaissance squads in the dismounted cavalry troop (C Troop), use HF in predetermined communications windows to report to their troop headquarters. In most cases, these communications do not enable timely or accurate reporting unless the unit is fortunate enough to observe the enemy near-simultaneously with their communications window. In the second method, a troop headquarters will establish HF communications with the Squadron as an alternate or as a contingency in the PACE (Primary, Alternate, Contingency, Emergency) Plan rendering it as an infrequently used or unused method of communications.

Common to both methods is point-to-point calling where two stations communicate solely with each other. This communication does not enable a rapidly shared understanding across the Squadron and therefore, does not serve as a suitable alternate option in a unit's PACE plan for a designated net. HF, however, supports the ability for all stations to hear the traffic and requires additional training for units to understand how to conduct a point-to-multipoint, or "ALL," call through Automatic Link Establishment (ALE).

Why units struggle with HF in a DATE Scenario

Units struggle to use HF in a DATE scenario because they lack the requisite level of training in antenna-theory and frequency selection to build an HF network sufficient to enable Mission Command. Operator training in these areas atrophied as units focused on bandwidth-intensive mission command systems and VHF/UHF line-of-sight (LOS) tactical radios. Five contributing factors below elaborate on why units struggle to make HF work.

HF Frequencies. In HF communications, the frequencies between 2 and 30 MHz all behave differently from frequencies in the VHF and UHF bands.

BG David S. Doyle received his commission in the Infantry from the United States Military Academy at West Point in 1993. His education also includes the Command and General Staff College (CGSC) and School of Advanced Military Studies (SAMS) at Fort Leavenworth and the National War College at Washington DC.

BG Doyle has commanded at the company level twice, battalion level, brigade level and has served as the Commander of Operations Group at the Joint Readiness Training Center (JRTC). BG Doyle is currently deployed in Iraq and serves as the Director of Operations, Combined Joint Task Force, Operation Inherent Resolve and is responsible for the synchronization of operations and effects across Iraq and Syria.

Spectrum managers often provide a unit with twenty different HF frequencies and consider this amount more than sufficient. Over seventy-five percent of these frequencies could be unusable because they do not fall within the range of 2 MHz to 10 MHz that enable HF Near-Vertical-Incidence-Skywave (NVIS) communications. One can visualize NVIS communications as water exiting a hose pointing straight up and splashing back down equally in all directions. This allows units to communicate near or out to 400 miles and can even enable units to communicate over large obstacles like tall buildings found in urban environments or over mountains. The usable frequencies within this NVIS range change between day and night because of the changes in the layers of the ionosphere that allow for it to refract signals back to earth. To support frequency selection, planners use a program called Voice of America Coverage Analysis Program (VOACAP) to provide a near-accurate report of which frequencies will support an area of operation for a specific duration of the day. Equipped with this analysis, units can make sure that spectrum managers are issuing frequencies that will support the mission.

HF Antennas. Units require different antennas to achieve different distances, depending on who a unit needs to contact. HF NVIS propagation can continuously support an entire area of operation out to roughly 400 miles. Units achieve this through VOACAP analysis frequency selection and through the correct selection of antennas to achieve high-angle take-off radiation. Bending an HF vertical whip antenna forward or backward for mobile operations or setting up a simple dipole antenna at least one-quarter wavelength above the ground for at-the-halt operation will achieve this high-angle take-off. Previous experience has shown that the NVIS AS-2259 antenna system, with its difficulty in tuning and easily lost parts, is not as effective as a dipole antenna. Units need not

LTC Ryan Seagreaves graduated from USMA in 1998 and was commissioned an Armor Officer. His operational experience includes command and staff assignments in 3rd BCT, 1st Cavalry Division as a Lieutenant, 3rd BCT, 1st Armored Division as a Captain, 3rd IBCT, 101st Airborne Division (Air Assault) as a Major, duties as a planner in II Marine Expeditionary Force at Camp Lejeune, NC, and 2nd IBCT, 4th Infantry Division as a Lieutenant Colonel, culminating in command of 3rd Squadron, 61st Cavalry Regiment. Institutional experience includes service as a Small Group Instructor in the Maneuver Captains Career Course, Chief of Tactics for Armor Basic Officer Leaders Course, and as the Cavalry Squadron Senior Trainer at JRTC. His operational and combat tours include 2 operational deployments to Kuwait, 2 combat tours in Iraq, and 2 combat tours in Afghanistan. He is currently a student at the US Army War College.

worry about which azimuth a horizontal dipole antenna is facing as these antennas radiate omnidirectional when placed in NVIS operation. This helps reduce setup complexity of the dipole. The azimuth of the dipole antenna will have a more significant impact when achieving much longer distance contacts such as 1000 or 2000+ miles away.

ALE "Individual" versus "ALL" Call. Given units want shared understanding; it is important that all stations on the net receive information at the same time. Automatic Link Establishment (ALE) is a technology that allows up to thirty-two individual stations to take part in a single ALE net that will automatically link stations together on the best frequency for that time of day from a pre-stored list of frequencies. ALE can link individual stations together or allow a station with traffic to connect to all stations through an "ALL" call. ALE has an added benefit of also allowing stations to transmit short text messages to each other. Units that do not understand how ALE works cannot use this technology built into every HF radio. It takes the guesswork out of knowing which frequency to switch to during the day or night and supports sending quick text messages.

Insufficient Training in Building an HF Network. The signal plan in the scheme of Mission Command should aim to achieve a shared understanding. In HF communications, units should avoid point-to-point "Individual" calling, and build an HF Network set to broadcast "ALL Call" to multiple receivers from a single station. While training an HF radio operator on how to place a call is relatively easy, ***building and maintaining*** an HF network in a DATE scenario is difficult. Building an HF network requires knowledge amongst operators across the formation on how to create an HF plan and programming that plan into the radio, understand HF wave theory, and propagation, VOACAP, and antenna theory and employment.

MAJ Matthew Sherburne is a Cyber Warfare Officer and student at the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas. He has previously served as an Assistant Professor in the Electrical Engineering and Computer Science Department at West Point, where he taught cyber security and digital communications to cadets.

MAJ Sherburne has also served as the Battalion Communications Officer for 2-325 Airborne In-fantry Regiment, 2nd BCT, 82nd Airborne Division during Operation New Dawn. He has also served as the Assault Command Post Platoon Leader for the 82nd Airborne Division providing en route communications for the Global Reaction Force and supported satellite communications during Operation Enduring Freedom.

Major Sherburne holds a Master of Science in Electrical Engineering from Virginia Tech and a Bachelor of Science in Electrical Engineering from West Point. In addition, he holds a CISSP license and an FCC Amateur Radio Extra Class license, callsign - KF4WZB.

Across all Cavalry Squadrons, JRTC OC/T's do not observe the required number of operators are not sufficiently trained to program the HF radios correctly, and adjust the plan, type of antenna, and antenna polarization daily as units move in a DATE Scenario to maintain an HF network that can enhance shared understanding. The U.S. Army Reconnaissance Center at Fort Benning, Georgia does a great job of training the usage of HF in reconnaissance missions. We strongly encourage units to send select Cavalry troopers to this school to bring back this HF knowledge and then to consistently use HF communications within their unit.

Battery Consumption for Dismounted Scouts. PRC-150s require two BA5590s at a time, double the battery requirement of a RT-1523 FM LOS radio. Unless a unit can get a sustained resupply of BA5590 batteries, it forces HF operators in dismounted reconnaissance squads on or near the forward line of troops to only use the HF radio during pre-determined communication windows to conserve battery life. Communication windows last twenty minutes every four to six hours. When units can communicate only during these communication windows, they are deficient in adhering to the Fundamentals of Reconnaissance to "report information rapidly and accurately." This limitation discourages units from using HF in their PACE Plan. These dismounted reconnaissance squads will need to consider solar-powered based rechargeable systems and extra rechargeable batteries in combination with using the lowest output power setting required to maintain contact to expand their communications windows.

Resources available to units

Foremost, units should read U.S. Army Doctrine that includes the Field Manual, Army Techniques Publications, Training Manual, Technical Bulletins, and Training Circulars that cover HF radio operation.

These include FM 3-55.93 *Long-Range Surveillance Unit Operations* Chapter 6: Communications [June 2009], FM 6-02 *Signal Support to Operations* [January 2014], ATP 6-02.53 *Techniques for Tactical Radio Operations* [January 2016], ATP 6-02.70 *Techniques for Spectrum Management Operations* [December 2015], ATP 6-02.72 *Multi-Service Tactics, Techniques, and Procedures for Tactical Radios* [May 2017], TM 11-5820-1501-13&P *Operator and Field Maintenance/Repair Parts for AN/PRC-150A*(C) [May 2013], TB 11-5820-1141-10 *Operator Manual for NVIS Antenna Handbook* [June 2008], TB 11-5820-1148-10 *Operator's Antenna Erection and Recovery Guide for HF Antenna System* [December 2005], and TC 9-64 *Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas* [July 2004].

The most important of these publications for Cavalry Squadron leadership and radio operators to know and understand is Chapter 6 of FM 3-55.93 and TC 9-64. Although there is the ATP 3-20.96 *Cavalry Squadron* [May 2016], ATP 3-20.97 *Cavalry Troop* [September 2016], and ATP 3-20.98 *Reconnaissance Platoon* [April 2013], these only briefly mention HF as a means to communicate. Leaders and radio operators can access these publications at https://armypubs.army.mil.

In addition to the doctrine, there are also many published articles on military HF employment. LTC (Ret.) David Fiedler and LTC (Ret.) Edward Farmer are the Army's most prolific authors on military HF usage publications. Their articles in the *U.S. Army Signal Corps Army Communicator* include the following: *Beyond-Line-of-Site Communications* (Fall 1983), *Skip the "Skip Zone": We Created It and We Can Eliminate It* (Spring 1986), *Russians on the Move – Near-Vertical-Incidence-Skywave* (NVIS) (Winter/Spring 1987), *On the Move - Mobile NVIS: The New Jersey Army* (Fall 1987), *Making it Work – Automated HF Communications For Nap-of-the-Earth Flying* (Spring 1994), *Planning for the Use of High-Frequency Radios in the Brigade Combat Teams and other Transformational Army Organizations* (Fall 2002), and AN/PRC-150 *HF Radio in Urban Combat, Mobility Favors Small Antennas*, and *HF Combat Net Radio Lesson Learned Again* (2004 Vol. 28 No. 4). The last three articles listed from the 2004 Vol. 28 No. 4 edition of the *Army Communicator* are the 'must read' for any tactical commander and his or her unit. Units can access the *U.S. Army Signal Corps Army Communicator* magazine online at the following address: https://signal.army.mil/index.php/resources/public-resources/army-communicator/267-archives. Once there, units can search for magazine editions to find the articles listed above.

The U.S. Army Network Enterprise Technology Command (NETCOM) maintains the Army Military Auxiliary Radio System (MARS) program headquartered at Fort Huachuca, AZ. This global system is comprised of multiple HF Gateway stations and numerous volunteer members with units that may contact to test their equipment and ensure they can make radio contact at short or long distances. Units may contact them at (520) 533-7072 to arrange a test HF radio contact.

Units can use the training documents and videos found on the LandWarNet eUniversity website https://lwn.army.mil and through the S6 Community of Purpose (https://nec.army.mil/portal/index.php/s6-cop-home). When users browse to the S6 CoP High-Frequency folder in the Documents repository, they will access numerous articles from Cavalry leaders such as MAJ Michael Hefti's paper titled, "The Need for Proficient Use of High-Frequency (HF) Communication within Cavalry Organizations," and training slideshows.

We also encourage units with authorized personnel to establish a Harris Tactical Communications Premier account at https://tcpremier.harris.com to access the latest software, drivers, and firmware for their HF radios and contact Harris for technical and training support. Having the latest software, drivers, and firmware is essential in achieving successful HF operation. Radio operators use computers to load the frequency and net plans into every radio. Units must ensure they have computers loaded with the software and drivers necessary to perform this function. Units can also leverage Communications-Electronics Command (CECOM) Logistics Assistance Representatives (LARs) to provide on-site support in training and assistance in ordering the correct component of end items (COEI) and basic issue items (BII) necessary to set up HF radios in vehicles and tactical operation centers. To test the HF skills of units, NETCOM hosts a low-powered HF radio competition called QRPX held at the end of every March. The Canadian Armed Forces host the Noble Skywave HF radio competition every October to test HF skills and multinational interoperability amongst NATO and partner countries.

Finally, we encourage Soldiers who want to further hone their HF skills to study for and earn their Amateur Radio license. This license is a clear way to show tested and certified knowledge in radio communications. Soldiers can then practice and hone their HF radio skills in their free time in a non-military setting. Units can find that local amateur radio clubs offer license exam classes and exams by searching this site http://www.arrl.org/find-an-amateur-radio-license-class.

RECOMMENDATIONS AND CONCLUSION

This article explains the Army's struggles with the tactical employment of HF communications in a DATE scenario through the lens of the IBCT Cavalry Squadron. The difficulties result from a lack of sufficient command guidance in ensuring regular training, maintenance, and usage of HF. The difficulties also stem from poor spectrum management in which units receive frequencies that do not support the propagation conditions. The fact of the matter is CTC's are now requiring the use of HF radio to prepare for Large-Scale Combat Operations in which units will almost assuredly face a cyber-contested environment in which the enemy will direction find and jam their VHF/UHF tactical radio communications. Units have the basic MTOE to support communications between all key leaders throughout all echelons. Unit commanders need to ensure that their MTOE has all the serviceable COEI and BII required for either base station, vehicular, or dismounted variants of their HF radios.

Units need to ensure they are using all available resources to conduct training on HF, so they know how to select the correct antennas and use the right frequencies to make HF communications work. Spectrum managers, just as operators do, need to better their understanding of how HF radio communications work to ensure they are issuing frequencies that will support the mission both during the day and at night. The primary advantages HF provides units in a DATE scenario are enabling Beyond-Line-Of-Sight (BLOS) communications and the ability to operate in a cyber-contested environment due to the inherent difficulties in direction finding HF communications. Commanders need to think about Mission Command in terms of the minimum essential traffic required to disseminate mission orders and attain a shared understanding to achieve decisive action through disciplined initiative.

Reshaping Intelligence Operations in the Cyberspace Domain

Major General (Ret.) George Franz
Lieutenant Colonel Galen Kane
Lieutenant Colonel Jeff Fair

Cyberspace has become the most active, contested, and congested of the warfighting domains. Both the new National Cyber Strategy and recent Department of Defense (DoD) Cyber Strategy describe an environment wrought with adversaries attempting to gain a military, political, and economic advantage over the United States (US). [1] Given the pace of operations and the rate of change in the environment, new ways of operating develop at a rapid pace. Although DoD has published Joint Publication (JP) 3-12 (Cyberspace Operations) that provides a foundation for understanding cyberspace and operations therein, the Army and Joint Force have a great opportunity (and requirement) to reflect the complexity and fluidity in this new domain and to more fully describe the level of conceptual and practical convergence between the land (physical), human, and cyberspace domains. The Army and Joint Force have the capacity to understand and detail these changes in the land and cyber domains and have the innovative leadership we need to integrate this convergence into our discussions, debates, concepts, and doctrine. The changes involved with the technology and the extent to which cyberspace is impacting the land and human terrain are significant even today. DoD must be bold and innovative to stay ahead of the threat and to take advantage of the tremendous potential that exists.

The critical component of the Joint Force and the Army being able to understand and operate in a converged environment is the Intelligence Warfighting Function. The current ability of intelligence to comprehend and describe this new reality is limited at best. Unless this gap is closed, DoD will continue to be at a decided disadvantage as technological trends continue to shape our world. The need for increased capacity and capability includes analysis, Intelligence, Surveillance, and Reconnaissance and building the ability to clearly articulate what is changing in the converged domains of land and cyberspace.

Major General (Retired) George Franz served as a Military Intelligence Officer at every level from Ground Surveillance Radar Platoon to J2 at the Joint Task Force level, including Command of USA INSCOM. He also worked in Cyber Operations positions as Commander, Cyber National Mission Force and as Director of Operations, USCYBERCOM. He retired in September 2017 with 33 years of active service and continues to support the MI Corps as a Soldier for Life.

To be clear, intelligence operations conducted in the cyber domain do not equate to intelligence support to cyberspace operations. Intelligence support to cyberspace operations build understanding and enable commanders at all levels to plan, equip, organize, and execute successful campaigns in areas determined to be in the national interest.

DoD Convergence Considerations

Former Commander, U.S. Cyber Command and Director of the National Security Agency, General (GEN) Keith Alexander, U.S. Army, described the convergence between the elements of the electromagnetic spectrum and cyberspace, which encompasses networks, signals, digital, analog, information, and data, as a full convergence of the signals environment. Specific to technologic convergence, GEN Alexander further warned of vulnerabilities and challenges created by the signals environment convergence, but this was just the start. From an Army operational perspective, the convergence GEN Alexander envisioned goes much further than just the electromagnetic spectrum and cyberspace, it also includes a full convergence of the land (including the human/cultural dimension) and cyberspace domains. Conditions now reflect a complete fusing of the human terrain with cyberspace. The extent to which people live in and through cyberspace, and the reliance humans now have on cyberspace to conduct a vast majority of routine activities, communications, and transactions. This means the Army, and especially as Intelligence Enterprise professionals, must develop the capability to operate effectively within this evolving operational paradigm. Our understanding of the cyberspace domain and its impact on future conflict must evolve beyond a rudimentary user-level understanding.

From a Unified Land Power or Army Operating Concept (AOC) perspective, this concept of convergence does not diminish the essential aspects of physical

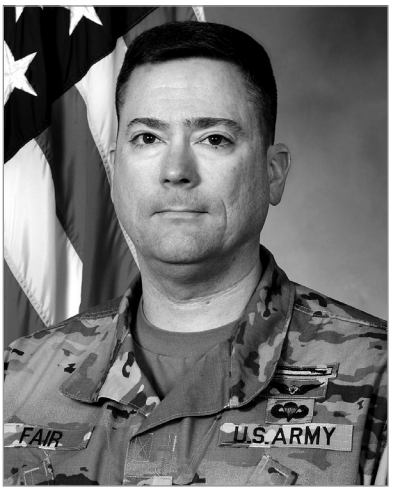
Lieutenant Colonel Galen Kane is a U.S. Army intelligence officer assigned to the Joint Staff J39 and recently completed the U.S. Army War College's Cyber Fellowship at the National Security Agency. He was previously the Commander of the 741st Military Intelligence Battalion and Deputy J2 for the Cyber National Mission Force, USCYBERCOM. He holds a BS from Indiana State University and an MA from Webster University.

land effects, nor does it change the fundamental elements of the land domain–the physical dimension – the Chief of Staff of the Army (CSA) General Mark Milley describes as the "crucible of ground combat" [2] is where the decisive aspects of land operations occur. The concepts outlined in the AOC establish the framework within which the Army will design its intelligence capabilities. In recent Congressional testimony, GEN Milley called for greater investment in cyber, Big Data, and networks and while the CSA's clear top priority is readiness, he indicated that "our number two priority is to invest in the technologies, organization, and doctrine that will allow us to maintain overmatch." [3]

A Converged Intelligence Approach

The U.S. Army and Joint Force are fully emerged in the cyber domain — every Soldier is a sensor, and these organizations have connected the individual to information networks in ways not previously envisioned. Equally fundamental to this land-human-cyber convergence is the nature of the terrain that we as an Army must operate in and are expected to understand and dominate. The depth of land-human-cyber convergence and the breadth of this condition across the globe means that wherever the Army and Joint Force will operate, we will deal with populations that are land-cyber converged. Every enemy, adversary, and competitor will operate in and exploit this converged land-human-cyber terrain to their advantage.

Doctrine already provides a structure with which to understand a converged environment. JP 3-12 describes the cyberspace domain as having three layers: 1) physical, 2) logical, and 3) cyber-persona. These three layers are used to define the environment, provide analysis on what resources the adversary utilizes, how it maneuvers, and operates throughout the three levels. What is clear from this is that the physical, as defined, encompasses land and land-based



Lieutenant Colonel Jeff Fair is a U. S. Army intelligence officer assigned to the USCYBERCOM/NSA Combined Action Group. He holds an MPA from the University of Washington's Evans School, an MBA from Hawaii-Pacific University, a MSSI from the National Intelligence University, and a BA from the George Washington University's Elliott School of International Affairs. He is a Ph.D. student at George Washington University's Trachtenberg School of Public Policy and Administration.

components. The aspect that requires additional development is the persona element. Intelligence professionals must take the initiative to capture the depth and breadth to which the human and cyber aspects are converged. It is possible for one individual to have multiple cyber personas. Due to the complexity of cyber personas, attributing responsibility or making an identification can be a very challenging task. In other words, the people among who we will operate are inseparable from the cyber-persona they live through.

For the Intelligence Enterprise specifically, this new operating model allows the Army to do a full and fundamental re-look of all current intelligence disciplines and concepts. The actions we take on land cannot be separated from those things we do in cyberspace–Army intelligence professionals must think of cyber-intelligence as a converged concept and related set of actions. All actions, analysis, and products must have a linked, fully integrated land-human-cyber core, which requires reconsidering all the intelligence disciplines, adjusting the intelligence cycle, and then pursuing opportunities to ensure a full appreciation of the land-human-cyber domain in our operational design.

Converged Army Intelligence

To inculcate the Army and the Joint Force into converged thinking, it should be integrated across the DOTMILPF. From an Army Intelligence perspective, the next place to reflect this new capstone concept could be foundational doctrine; Army Doctrine Reference Publication 2-0 (Intelligence). The following are ways that our doctrine could describe each intelligence discipline and its relationship to cyberspace:

- **All-Source Intelligence:** In a converged environment, all sensors must be integrated across multiple domains to build a reliable, accurate picture.

This begins with creating all source analysts that possess a detailed understanding of cyberspace. A July 2017 assessment by the United States Army Intelligence Center of Excellence determined that "to propose viable and worthwhile threat courses of action in cyberspace, all-source intelligence analysts require a true understanding of the Cyberspace Domain and the kinds of operations that threat actors perform in cyberspace to achieve different objectives." [4] The approach to all-source intelligence must expand to incorporate the significant information available that pertains to the cyberspace domain, particularly network data that is currently seen as defensive or administrative. All sources must include operational reporting from network operators and administrators, just as operational forces report combat information on the ground.

Just as every Soldier is a sensor, then every network sensor must be integrated as a potential intelligence sensor. The Cyber ISR system must incorporate network data collected from the wide array of security and information assurance sensors such as the Host Based Security System and others. Network operators must also be more effective in reporting a threat or potential threat activity, using the established report formats and mechanisms that will enable ingestion of combat network data into the intelligence processing, exploitation, and dissemination (PED) enterprise.

- **Signals Intelligence (SIGINT):** The signals and information environments are fully converged, although conventional legacy communications that, in many cases, are used to defeat or protect from our current signals collection capability must be addressed and updated. Even as cyber forces develop their combat (Title 10) collection capabilities, SIGINT will remain the most vital component of the ISR system. SIGINT is recognized as a primary driver for operations within the cyberspace operating environment, but the fusion of all sources of intelligence is critical to disrupting or defeating adversaries.
- **Human Intelligence (HUMINT):** Almost every human on the planet now has multiple cyber-personas to match their physical/actual identity requiring that all HUMINT operations account for the whole person/persona synthesis as a target. The tactics, techniques, and procedures (TTPs) for all aspects of HUMINT operations must integrate activities in both the land and cyber domains. As much of valuable intelligence information is now passed via electronic means, the cyberspace aspects of HUMINT will become the main effort, with physical activities becoming a deliberate enabler for virtual/cyberspace access development.
- **Open-Source Intelligence (OSINT):** Open source data is becoming the timeliest and potentially, the most lucrative form of intelligence as rate the level of data produced by individuals increases daily. Given the difficulties in accessing encrypted data and recognizing the effects of unauthorized public disclosure of classified information, we will have to rely on more widely accessible data in this new era. Our ability to collect process, exploit, and disseminate social media information, open source data, and commercial

and personal imagery, will be a critical aspect of Indications and Warning, Intelligence Preparation of the Battlefield, developing situational awareness, and cueing more sensitive and precise collection systems.

- **Counterintelligence (CI):** It is also clear that the enemy is fully exploiting cyber-space and the weaknesses in our network defenses to their advantage. Everyday threat intelligence services and other adversaries attempt to penetrate our networks and collect valuable information. In many cases, the enemy uses personal contact and HUMINT targeted spear-phishing as the means to establish cyber access and, while the days of dead-drops and microfilm are not entirely gone, the vast majority of collection against the U.S. Government and Army is accomplished through cyberspace. The Army must take a hard look as it executes CI operations, how it trains and employ the force, and how it establishes much tighter links between the network operators, defenders, and CI agents. While there is still a vital need for covering agents, face-to-face contact, threat awareness briefs, and walk-in reporting, intelligence organizations must expand their presence and operational capabilities to defeat the enemy pouring through the cyber gap.
- **Geospatial Intelligence (GEOINT):** This discipline will continue to play a vital role in cyberspace intelligence, with the cyberspace physical aspects being most commonly associated with GEOINT. Geography and location are still core elements of Unified Land Operations and the AOC and, as long as the current model of international governance recognizes land borders, the Intelligence Warfighting Function will provide the geographic location and precision in targeting required for military operations. To ensure effective geospatial support to cyber operations, we must develop the means to geolocate network activity, to track actions in both network time and space, and establish the means for PED that can support decision makers and operations.
- **Targeting:** From a practical perspective, targeting comes down to our ability to effectively achieve effects and impact in cyberspace in support of combined armed operations, across multiple domains. We must be able to target for precision Intelligence, Surveillance, and Reconnaissance, CI, Information Operations, and across the full range of military operations. The Department of Defense has spent years developing the TTPs for targeting in support of combatant command operations, and this remains an incredibly difficult task.

The Convergence Imperative

As early as 2013, BG Jeff Smith, U.S. Army, captured the concept of land-cyber convergence, but his white paper was ahead of its time. [5] Six years later, the Army has moved forward with the creation of the Cyberspace Operations Branch, the establishment of the Army Cyberspace Center of Excellence, Army Cyber Institute, and the growth of Army Cyber Command (ARCYBER) as a fully capable Army Service Component Command, validating

much of BG Smith's work. In addition to the publication of JP 3-12, the release of Field Manual 3-12 (Cyberspace and Electronic Warfare Operations) in April 2017, and the AOC, as well as the increased level of awareness of cyberspace across the Army and Joint Force has established conditions that allow a much more complete and holistic approach to a land-human-cyber concept. We should be aggressive and bold in our approach, or we risk failing to provide useful intelligence to support and drive operations in the complex environment as it now exists. We must rapidly proliferate this concept across Army and Joint Force doctrine and concepts. To drive successful operations in the cyber domain, Intelligence must continue to be Always Out Front.

DISCLAIMER

The views and opinions expressed in this paper and/or its images are those of the author(s) alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DOD), U.S. CYBERCOM, or any agency of the U.S. Government. Any appearance of DoD visual information for reference to its entities herein does not imply or constitute DOD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

NOTES

1. The White House, "National Cyber Strategy," Washington, DC, September 20, 2018. United States Department of Defense, "2018 Department of Defense Cyber Strategy Summary," Washington, DC, September 2018.
2. Chief of Staff of the Army General Mark A. Milley, "39th Chief of Staff of the Army Initial Message to the Army, " memorandum for the U.S. Army, Washington, D.C., September 1, 2015.
3. Sydney J. Freedberg Jr., "Gen. Milley to SASC: World Getting Worse, Army Getting Smaller," July 21, 2015, https://breakingdefense.com/2015/07/gen-milley-to-senate-world-getting-worse-army-getting-smaller/, accessed May 10, 2018.
4. United States Army Intelligence Center of Excellence, "Intelligence Support to Defensive Cyberspace Operations and DoD Information Networks (ISDD) Assessment," Fort Huachuca, AZ, July 17, 2017. 37. (Classified).
5 U.S. Department of the Army, *The U.S. Army Land Cyber White Paper* 2018-2030, Fort George G. Meade, MD: U.S. Army Cyber Command/2nd U.S. Army, September 9, 2013.

The Cyber Defense Review

Professional Commentary

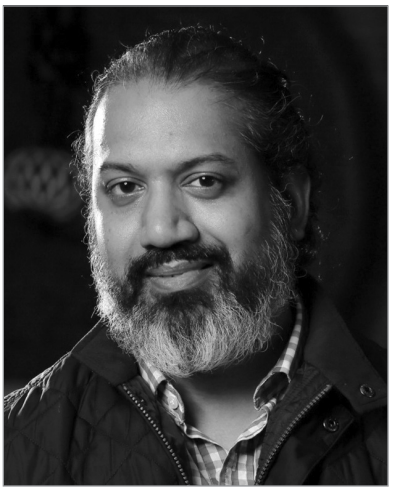
Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s

Oz Sultan

Over the past decade, social media has become an abusive component of the general media that we consume daily. In many cases, social media precedes and precludes traditional news mediums, by getting information out early or by providing detailed accounts of what is happening on the ground across the world.

What started out as social media users, influencers, and netizens capturing everyday happenings and reporting them in real-time (from 2007 to the present), evolved to include complex and organized propaganda systems by 2009. [1] Early propaganda systems involved state-sponsored propaganda sites presented as independent social media handles. State-sponsored disinformation began with Russian troll activism in Finland in the early 2000s. Infowar expert Dr. Saara Jantunen's book "Infosota", published in 2015, details the complicated networks of troll houses and blogs that constitute the concerted Russian infowar effort. [2]

In the first stage of the Ukraine conflict, Russia seized the Crimea, and Dr. Jantunen along with Finnish journalists and Finnish military researchers covering the conflict saw themselves slandered by a mixture of Russian trolls, Russian bots, and Russian disinformation blogs. Jessika Aro, one of the journalists investigating the trolls, was the most impacted as attacks targeted her home, phone, and workplace. [3] Finland has been able to keep Russia propaganda mostly at bay through legal attacks on the Russian disinformation campaigns that were run in-country by troll farms, [4] and by developing and supporting a compelling counter-narrative. [5] Finland's counter-narrative was launched in 2015 and is a top-down, bottom-up strategy that involved the engagement of 100 officials across various levels of government to analyze and map the spread of disinformation across their country. This strategic engagement included the participation of the FDR Center for Global Engagement at Harvard, for Finland to understand virality of disinformation. [6]



Oz Sultan is a tech, marketing and blockchain Industry veteran with 20 years' experience developing innovative solutions for brands and Fortune 100 companies. He is also at the forefront of American Muslim affairs, active in diplomatic and interfaith engagement.

Over the past ten years, Oz has leveraged social media signaling and analysis of trend and social media data to focus on Big Data analysis and how patterns can aid in solving complex problems. Oz has developed a Digital Anti-ISIS framework and counter-radicalization and disruption methodology for stopping online terror. In 2016, he was a counterterrorism, social media and Big Data advisor to the Trump Campaign. He is a regular contributor to i24 News, TexasGOPVote, The Ish, and Newsmax.

Oz currently consults in the Blockchain, Crypto, Cybersecurity and related CT arenas. He is a Board Member of the Homeland Security Foundation of America (HSFA); a Senior Fellow of the Council Board of Exchange; and a Senior Fellow at the National Minority Technology Council.

However, what the attacks on Finland have underscored is the larger Russian agenda to target western Europe – specifically Germany. The case of the false 'Lisa Story' in Germany from January 2016 is often cited as a textbook example of Moscow's modern information capabilities. Russian-language media reported allegations that a 13-year old Russian-German girl had been raped by migrants in Berlin before local authorities had time to verify the information. Those Russian reports were then picked up by mainstream news media in Germany and elsewhere. The false "Lisa Story" played out significantly across social media beyond Germany, most notably on Facebook, Twitter, and Reddit, where it was shared and re-shared with a significant impact. In the 'Lisa Case' we see evidence, for the first time, of several Russian elements of influence that are described in this article working in a coordinated way:

- A journalist from the First Russian TV channel picked up the case of the Russian-German girl and brought it to the main news in Russia;
- Russian foreign media like RT, Sputnik, and RT Deutsch reported on the case;
- Social media, as well as right wing groups, distributed the information on the Internet;
- Demonstrations were organized via Facebook involving representatives of the German-Russian minority (Deutschland Russen) as well as neo-Nazi groups;
- Russian foreign media in Germany reported from these demonstrations, which brought it to the German mainstream media;
- Finally, at the top political level, Russian Foreign Minister Sergey Lavrov made two public statements about his concerns about the inability of the German police and legal system to take such cases seriously because of political correctness. [7]

The evolution of Russian propaganda attacks from 2010 to 2015 was a testing ground for more massive campaigns launched against Germany and subsequently America. The false "Lisa Story" demonstrated how Russian propaganda stoked social media outrage and was supported by official disinformation that resisted challenges to the story with ambiguity, thereby rendering it as 'factual' in the minds of the audience it is intended to influence.

Understanding Online Propaganda and Amplification

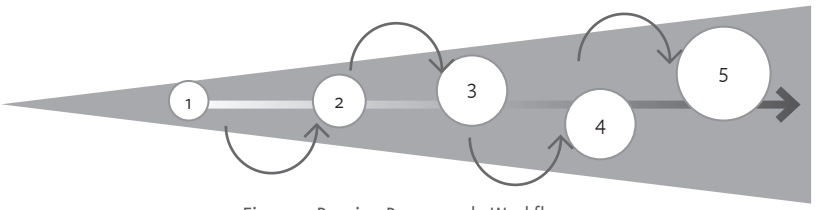


Figure 1. Russian Propaganda Workflow

The basic workflow of how Russian propaganda is developed, disseminated, and amplified is highlighted in Figure 1. The challenge with disrupting this workflow is one of a lack of preparedness on the part of many entities that are targeted: nations, politicians, corporations, and individuals. The steps of the Russian propaganda workflow are as follows: 1. Initiating incident (Lisa example) 2. Press or social validation 3. Foreign power amplification (Russian leadership commentary, for example) 4. Social buzz and shares 5. Social reshares and propaganda are taken by fact by people consuming it on social channels.

That the Russian model is partly leveraged by other state actors, such as Iran and China, which underscores the increasing challenge before the US and other democracies. We see conflation online between disinformation by state actors (and their respective social media strategies) and the difficulty of real-time media reporting. The latter is often becoming the tool of disinformation campaigns in their hurriedness to be the first to report. [8] The Defense Intelligence Agency (DIA) noted that:

> Russian intelligence services, including Russian military intelligence (GRU), have been increasingly involved in carrying out cyber operations abroad, as we have seen in the United States, in efforts to sway the 2017 French presidential election, and in attacks against Ukraine's power grid. The Kremlin is further developing these capabilities and its capacity to carry out information warfare, or what it calls "information confrontation." Moscow views control over the information sphere as crucial to influencing, confusing, and demoralizing an adversary, and the weaponization of information is a key element in Russian strategy. Russia employs a full range of capabilities, including pro-Kremlin media outlets and websites, bots and trolls on social media, search engine manipulation, and paid journalists in foreign media, to sway Western attitudes toward Russia and in favor of Russian governmental objectives. [9]

To challenge and disrupt Russian and state sponsored disinformation, as well as copycat campaigns leveraged by other foreign state actors, it is important to rapidly identify the false narrative stories. These are generally posted by a little known, unknown or subversive news/information site and mirrored in many languages across the Internet. These anchor stories, such as the "False Lisa" story, work like a signal that gets retransmitted through several repeaters. Disruption of these stories or weaponized content should actively involve the social media platforms that facilitate their dissemination. However, what we've seen in recent years is a reticence by Facebook, Twitter, Instagram, and WhatsApp to follow through.

If we are to be successful in countering the false narratives and propaganda, we need to be developing social media countermeasures and Standard Operations Procedures (SOPs) to parallel the deployment of personnel and ground communication systems. For forward deployed forces, this means developing a new social listening SOP that goes across traditional social channels (Facebook, Twitter, Instagram, Reddit, Snapchat, WhatsApp, Groupme, Voxer), new social channels (Telegram, Signal, Discord, Line, Kakaotalk, Weibo, Wechat, Coco, SOMA) and emerging crypto social channels (Steemit).

A simple model for analysis can be built upon the social mapping leveraging a tool like Gephi (https://gephi.org/) or Centrifuge (http://centrifugesystems.com/), which allow for an analyst to start mapping the social sharing across social networks and amongst power users or influencers. There are also a host of python and codeable tools out there, such as Graphtool (https://graph-tool.skewed.de/) and Carnegie Mellon University's GraphChi (https://github.com/GraphChi/graphchi-cpp). The key is to look for the 'social seed' or anchor piece of propaganda that started the sharing storm and then track where it jumped networks and who was endorsing it. Additionally, there are two factors that empirical analysis typically misses: velocity and popularity.

Velocity can be calculated based upon the speed by which a Tweet or series of Tweets spans different social graphs. Popularity is more imprecise math but can be roughly assessed by analyzing influencers (roughly 5k or more followers) and super influencers (approximately 100k or more followers) [these numbers also vary by network] that engage with or share the propaganda content. Generally, once you understand the amplifiers of specific types of propaganda, it becomes easier to develop a campaign through which you can respond to influencers or power users through sub-Tweets and structured social posts.

The challenge comes once the propaganda is picked up and spread by a mainstream news outlet and shared as either a 'story' or 'opinion' piece. This is further complicated by endorsements from Russian of other state agents or officials who are endorsing propaganda they issued in the first place.

From online propaganda to online terror

The modern terror recruitment network has moved beyond the 1980s, 1990s and early 2000's models of passing a terror training manual in the style of an 'Anarchist's cookbook' coupled with destination terror training camps. Beyond Russia, we are seeing parallels in online terror recruitment and influencing models. However, with terror recruitment, a piece of propaganda that is already widely disseminated or a terror attack that validates propaganda is used instead as a propaganda seed.

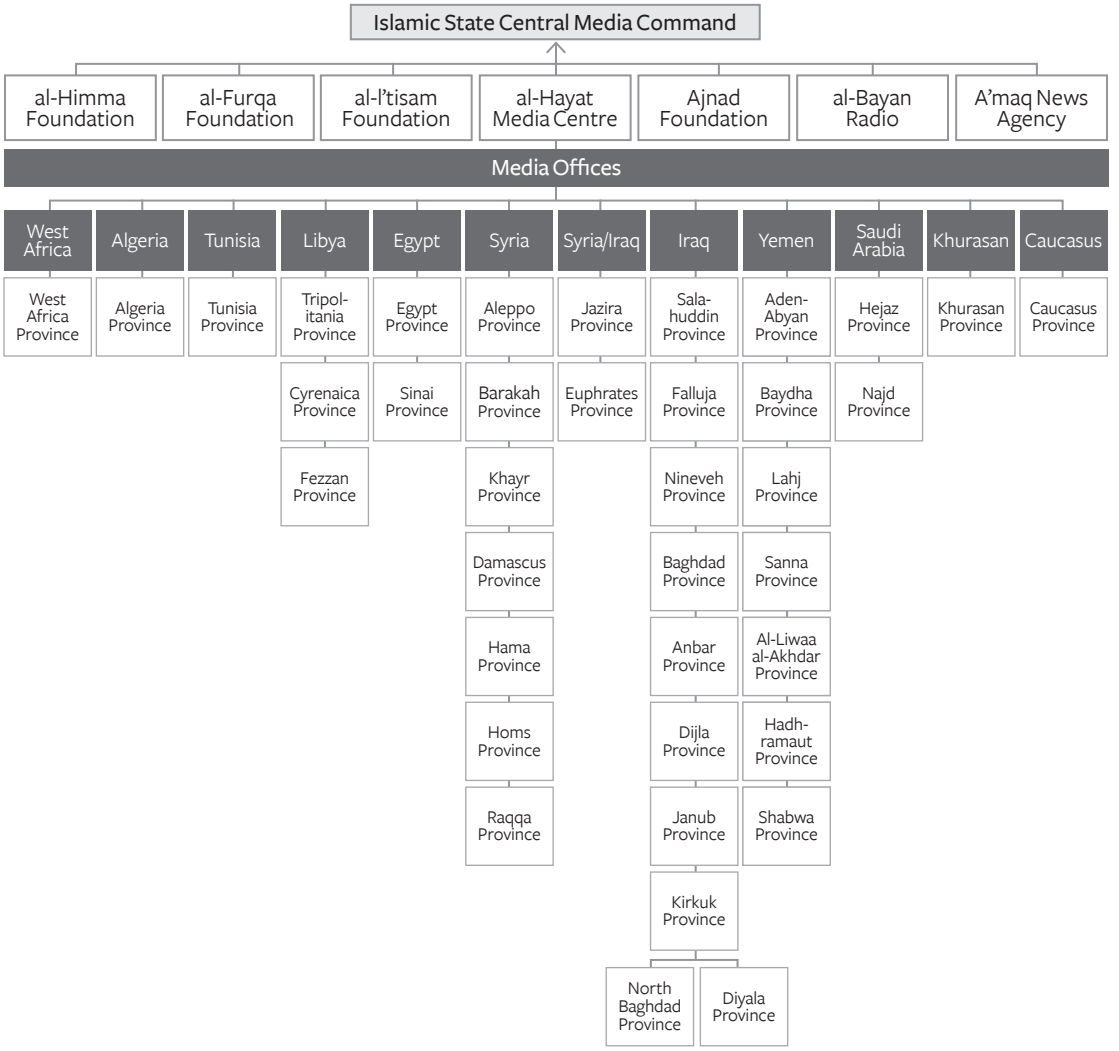


Figure 2. The ISIS Social Media Engagement Network Model (SEN) Source: Quilliam

ISIS's Amaq news agency has not only launched video and audio news but guides and training, as well. These are disseminated across a broad range of sites making suppression and remediation complicated. As of 2016, ISIS has been leveraging a complex content development and dissemination system coupled with online recruitment. The model below illustrates that Amaq and Al-Hayat – the most reported on ISIS news agencies, in the west, are only a small part of a vast network of online propaganda and influencing and recruitment efforts. As these networks are well entrenched across many conflict regions in EMEA (Europe-Middle East-Africa), while battlefronts change, the online presence persists.

Attacks by the US-backed Syrian Democratic Forces (SDF) in Syria have decimated ISIS Syria online operations, but many have just moved outside of Syria. Further, with the cross-pollination that has occurred between ISIS and al-Qaeda, cross-group insurgency is on the rise especially in complicated areas like Yemen and North Africa. SOPs for the assessment of ISIS and al-Qaeda related activities before ground incursions or tactical assessments should begin with a review of online engagement, which is made easier with tools like Livemap (https://isis.liveuamap.com/).

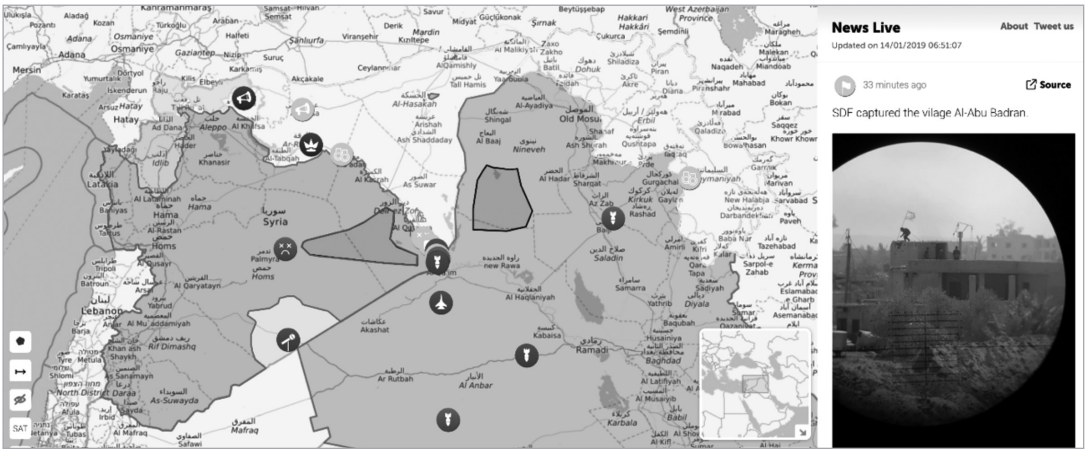


Figure 3. ISIS Social Engagement Network

Covering most of Middle East and North Africa, Livemap is a good start point in mapping what is going on in real-time, as well as what is being shared by ISIS and their SEM (Social Engagement Network). Social listening and mapping tools to understand where their propaganda is being disseminated are still necessary to map a specific incident. Typically, you can look to an attack or recent incursion and the messaging that is shared on Twitter, Telegram, and Signal. The challenge, however, is that the latter two social networks often have private groups that are invite only, which requires a bit of reconnaissance. Popular gaming platforms with chat on Xbox, PS4, and Nintendo Switch should also be kept in mind and analyzed based

on the frequency of gaming related tweets within a specific geographic arena. Generally, this is an indicator of where ISIS may be prospecting off social media networks, as well as areas for development of new SOPs.

Chatbots and Botnets

Chatbots and the development of automation bots in the 2000s have given rise to some unforeseen complexities, related to both social media and cybersecurity. What began as a method to automate volumes of standard responses to customers, as well as to provide an automated channel for customer engagement, has given rise to social media manipulation, distributed conversation attacks, and online mayhem. Similarly, Internet bots are automated programs that allow for the execution of a variety of tasks online have given way to networks of bots that can be rented like cloud hosting for any conceivable use under the sun.

The impact of these shifts is significant: In 2016, early ISIS botnets were deployed across Twitter [10] and operated much the same way as Russia, North Korea, and dark web hacker networks where attack networks can be rented, as easily as you or I could rent an Internet web service. In this environment, compromises range from simple scams across social media that request money or cryptocurrency [11] and then continue the scam to automated Distributed Denial-of-Service (DDOS) campaigns that leverage malware, brute force attacks, and propaganda dissemination.

DDOS Campaigns

In March 2018 Akamai reported that:

> On March 1, Akamai defended developer platform GitHub against a 1.3 Tbps attack. And early last week, a DDOS campaign against an unidentified service in the US topped out at a staggering 1.7 Tbps, according to the network security firm Arbor Networks. Which means that for the first time, the web sits squarely in the 'terabit attack era'. [12]

The significance of the power of these attacks means that we are now facing attacks that can overload and compromise network backbones and Tier 1 data providers. It is also the tipping point for the rise of DDOS attacks on the Internet of Things (IoT) and networked devices. Many of these new attacks target DNS or front-end web services, areas of the network that may be outsourced or less securitized in a cloud environment.

In 2003, I dealt with the rerouting of one million-page requests an hour through a home DNS server, after the Fortune 100 company I was working for experienced a catastrophic DNS failure. Had this option not been available, we would have looked at close to $1M in losses within a week. With new, cheap and difficult to trace Botnets, we now face rogue attackers who can erase their tracks, as quickly as they spooled up an assault.

Additionally, as IoT devices (which are mostly insecure or unsecured) start to become more mainstream, we face a new wave of risks that will affect every US military installation.

In many cases, it's not network deployed IoT devices (which need their own SOP) that are at risk for hacking; it is Bluetooth and PAN (Personal Area Network) attached devices like a Fitbit or an Apple watch or off-brand headphones with heart tracking that give away the location of military installations. [13] IoT devices are increasingly at risk for botnet hijacking. A secure protocol limits certain types of devices from FOBs but a more secure strategy is to develop SOPs that manage both networked and personal IoT risks.

Propaganda Dissemination

Similar to Russia's leverage of social media, the rise of bots within the social media ecosystem has had a chilling impact. As the propaganda models mature and become further decentralized across a broader geographic landscape, the risk is the speed and efficiency with which botnets can "vouch for" false narratives. A Tweet that starts as propaganda can be timed to be re-Tweeted and reshared by bot accounts that have thousands of followers and have been engaging in similar conversations for months before they are leveraged. If these accounts are not flagged or filtered they will continue to exist as a nexus that can share and reshare propaganda, false flag operations or disinformation.

Take for example propaganda bots impacts in Mexico [14] which have had chilling effects on influencing and shaping what people believe. The botnet phenomenon is also a technological leap in the impact of content dissemination and political or personal influencing. Consider bots as an amplification of the radio by a multiple of at least ten times. As botnets become cheaper, simpler to rent, and more accessible through cryptocurrency, a review of non-state and regional actors with social media fluency should be conducted to assess a threat baseline. Research teams that can analyze specific bots and bot attacks become extremely necessary as more organizations become impacted by bot attacks. [15]

When deploying social listening tools for active operations or assessing a given geographical landscape; once the general nature of daily conversations patterns is known and when propaganda shares can be tracked, it comes to either active disruption with owned or contracted social media handles, or a mass reporting action, which, while time-consuming, will deactivate the bot accounts. Another alternative to get a block of bots shut down rapidly is to work through representatives from Facebook, Twitter, Instagram, Telegram, Signal or other social platform's Fraud/Terror or Hate management teams.

Developing Digital Counter-terrorism (CT), IOT, Social and BOT SOPs

Bot technology is not a new thing. If we look back to punch card automation on IBM Systems and the architecture of virus software, we see a software process that can be automated to achieve the desired goal. The difference today lies with the number of bots, their coordination, and the efficiency with which they operate.

It is crucial to develop a SOP that accounts for bots and is a guide for specific types of bots within a known scenario. For example, if you want to prevent undesired social or data sharing of secure facilities or military installations, it may be necessary to require personnel to leave all personal IoT devices before coming to work or deploying. For cell phones and personal data devices, a VPN coupled with portable Faraday cages may be a simple solution to allow communications to their families and friends, while maintaining security. Why? Because if the Russians have started to ban their soldier's cellphones for fear of social media exposing deployments, we should be taking a few more cautionary steps. [16]

For SOP development, first, establish the scenario you need to protect. For example:

1) Restrict personal data sharing by personal, cellular or IoT devices on an installation or campus.
2) Eliminate the risk of hacking for network deployed IoT motion sensors deployed within a 5-mile radius.
3) Target a Russian or ISIS botnet operating within a specific theatre of operations.

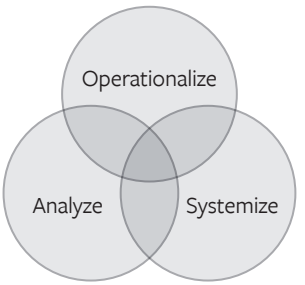


Figure 4. SOP Development

1. Analyze

For each scenario above, assess the following:

a. **Players:** Who is involved? Who is in command and requires reporting?
b. **Protocol**s: What are we trying to protect, defend against or prevent?
c. **Devices:** Are the IoT devices personal or public? What is the range of these devices? Who manages them? Who is responsible for securitization? What authorizations are needed?
d. **Bots:** Use standard network security SOPs to define penetration vulnerability for each scenario, for as many scenarios that exist.
e. **System:** Create a base protocol, process, stakeholders, escalation and implementation guide.

2. Systemize

a. **Define the boundaries:** Who does this impact? When does it need to be in effect? How will it be enforced? What are the compliance guidelines and the non-compliance ramifications?

b. **Establish the system:** Develop a basic guide; document and perform a test implementation. Iron out the kinks and repeat.

c. **Measure the results:** Establish metrics, cases for upgrades or modifications to the process and develop an approval process.

3. Operationalize

a. Deploy and perform a final test review.

b. Standardize across related or impacted operations.

c. Scale as necessary.

d. Perform periodic reviews to ensure the process is effective.

e. Assess metrics and report periodically.

f. Identify best practices that can be shared as SOPs for similar implementations or JSOC operations.

Cyber Risk Planning and Assessment

With the number of cyber-attacks and hacks that have occurred over the past 24 months, including the Marriott hack of 500 Million user accounts and recent compromises of critical infrastructure around the Tribune companies, it's time to start re-assessing risks from corporate civilian cloud infrastructure within the military and defense space. The NJCCIC (New Jersey Cybersecurity and Counterterrorism Information Cell) has noted the risks of China's Flusihoc bot network as well as those of, Iran, North Korea, and Russia. What last year's hacks underscore is an increased need to secure military systems that leverage cloud or public/hosted systems architectures. Those hacks also point to a change in the DDoS and Botnet attacks. Whereas previously, attacks were focused on disabling systems and locking data, these new attacks are designed to compromise cloud infrastructure and backend systems. [17]

The impact of this change is twofold. Instead of locking or stealing data, a successful attack could provide a foreign intruder access to critical publishing systems. As the social media and Russian propaganda machine have illustrated, this could prove catastrophic if it leads to mass dissemination of content. Consider the impacts during an election cycle or maritime conflict overseas.

The complexity of disinformation campaigns and hacks lead to threat scenarios that range from the risk of a news outage or a propaganda push during a foreign military campaign or attack. This is an increasingly real threat scenario that deserves further modeling, especially given China's recent militarization of the South China Sea.

To develop new SOPs for these risks, we need to establish cyber baselines, both for civilian linked and military deployed systems. Intel gathering from social media and public/dark web sources needs to become an ongoing passive process. Smaller attacks are often the precursor to larger scale attacks, and DDoS attacks need to be monitored to understand the trends of attack software and ransomware. Today it could be Ryuk, tomorrow, it could be reuse of WannaCry targeting unprotected medical devices or hospital infrastructure. [18]

Part of the problem is that across the U.S. Government and public technology infrastructure, we have a broad range of operating systems and control software ranging from early Windows and DOS variants to ACOE water table collection systems that still run on dial-up accessible UNIX systems. Healthcare and power generation systems add another layer of complexity, as they are easily targeted, and simply due to luck have not been the subject of a large-scale ransomware attack.

The US cannot continue down this perilous road. Security should involve assessing the age and penetrability of systems across a campus, FOB, enterprise, MAN (Metropolitan Area Network or City) or National/Global Network with rapid identification of unsecured network segments, as well as outdated or at-risk systems. This complexity will further increase with the development of Smart Cities that have layers of distributed IoT networks.

Smart Cities themselves will pose a more significant challenge, as the deployment of quantum computers improve the quality of life, reduce pollution and congestion, and extend major impacts to the battlefield of the future. This will bring a flurry of changes with the SOP process above and aid in planning. Cyber vulnerability assessment SOPs should follow existing and known protocols across military services, with updates made, at least quarterly, to the known universe of risk as well as new risks that stem from the overlap between military, MAN, developing Mesh power systems, cellular and civilian platforms and technology systems (social media, civilian to military-connected payment and data systems), as well as data vulnerabilities stemming from data stores of critical or vulnerable information.

The Cyber Risk Planning Ecosystem

Assessing the specific risk exposure for your scenario should begin with an analysis of your existing SOPs and a review of additional areas of concern that emerge from the risk ecosystem presented above. Full-scale cyber risk planning should involve a review of affected systems within your ecosystem – and the development of a mind map, as above. Once this is completed, begin with reviewing your systems risk, data risk, and then, personnel risks.

Lastly, by the mid-2020s, expect many legacy technology systems, databases, and platforms to begin or be at the end of their life. The ramping down and archiving of these systems presents a future risk, as simple hacking techniques such as "dumpster diving" when a hacker goes through a system's garbage can have major impacts if these systems are not sanitized and properly disposed of. The same applies to their data, which while less sensitive to you, may still be valuable to a less technologically advanced adversary.

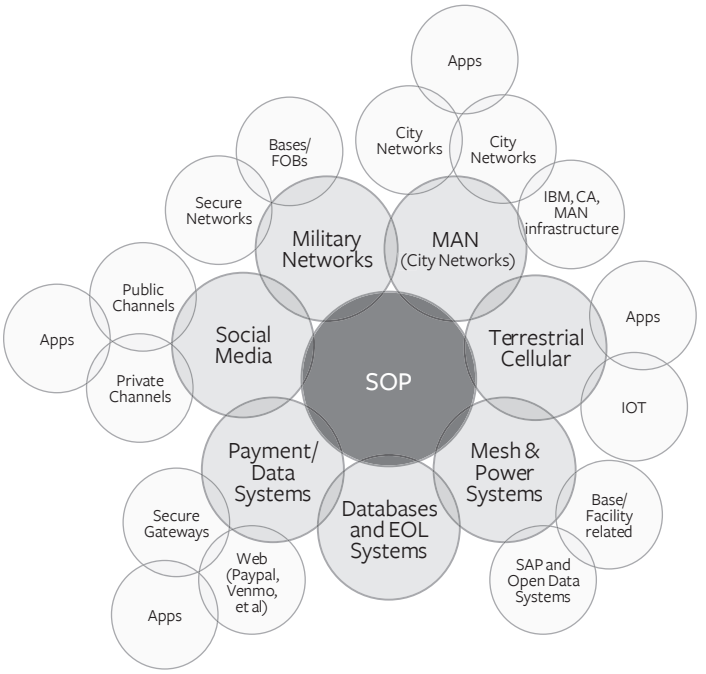


Figure 5. Risk Ecosystem

The Path from Cyber to Cryptocurrency

Cyber-ransom and cyber-attacks have rapidly opened the door between the cyber world and the crypto world. What began as global crypto-ransom attacks (WannaCry, Petya, NotPetya, Ryuk, et al.) [19] in 2016 and 2017 have given way to regular full-scale attacks across the Web, against the Web backbone, and even edge hosting services used for scaling to handle large customer requests.

The crypto world itself has also grown from a nascent environment of digital currency hobbyists to a multi-billion-dollar industry that will scale to the trillions, as developing countries begin reconciling their cross-border payments in Bitcoin and as large institutional players enter the market. This new market presents many opportunities and challenges as black-market transactions that have historically been done in cash have rapidly moved online and to the dark web.

The rise of crypto has also created cascading problems in human-trafficking, organ-trafficking and black-market sales of arms and embargoed goods. Iran recently presented a new dimension when they leveraged Bitcoin to bypass US sanctions. ISIS has long leveraged crypto to finance their insurgent operations across EMEA. Crypto exchanges themselves present another challenge as they are moving from startup style operations to larger scale daily transactions, so they are often subject to hacks and exposure, such as the release of information on 450,000 customers at CryptoMama. [20]

Global Crypto Implications

In South America, Venezuela has already begun settling cross-border payments with Bitcoin. [21] Several regional cryptocurrency systems have risen in Africa, facilitating both regional transaction systems and a reduction in cross-border payment expenses. Dubai has been focusing on a crypto trade zone that allows for Security Token Exchanges, while DATA [22] (US domestic Blockchain policy organization) is working with the Wyoming state government on both domestic crypto laws and the definition of crypto as currency. Simultaneously, Indonesia has moved to classify crypto as a commodity. [23] What does all this mean? The role that hard cash, black money, gold, and commodities played in the past is being rapidly challenged and replaced by digital currency and commodities.

The near-term implications of crypto are that new payment and commodity platforms are in play and need to be assessed as the world begins to move from paper and credit-based payment systems into digital payments and the Blockchain. The longer-term implications are yet to be determined. However, the global impacts of shifting currency and payment systems will alter how we conduct everything from remittances to forensic data analysis, to day-to-day operations across both civilian and military sectors.

The Blockchain

As China and Russia have challenged countries in EMEA, the US has begun to take steps to develop and deploy technology that moves it ahead globally. The Trump Administration has rapidly facilitated the assessment and development of Blockchain systems that will be evaluated within Opportunity Zones across the US, allowing for evidence-based research on a national scale. Within the military and civilian-related arenas – we need to consider the applications of the Blockchain, as well as the opportunities it presents both today and in the future.

Blockchain Use Cases

The Blockchain is simply a secure, immutable database that allows for transactions, queries, applications, and tools to be built while eliminating all middlemen and extra hands in the process. It creates is a system of trust that leverages frameworks (called smart contracts) which allow for process-based or automated transactions. The use cases for the Blockchain are infinite – as is the value that is created with new Blockchain deployments

and Blockchain systems. However, for simplicity sake, a few examples to clarify the value of Blockchains.

Weapons Management

Take for an example, the challenges of monitoring, tracking, and managing 1,000,000 H&K rifles deployed across several FOBs in three theatres. Today this is done with a mish-mash of technology and paper-based solutions that often tax both workforce and systems. Now consider a Blockchain based solution that was deployed leveraging an Ethereum or XYO based technology, which could place an encrypted, globally accessible tracking tag on every weapon. Then consider that the tags could be integrated to allow for missing, stolen or captured rifles to be deactivated or deauthorized from use. The system allows for constant inventory, management, authorization or archival and reduces cost, complexity, and workload.

Healthcare Records/Combat Medic Matching

In an operational theatre, access to a unit of blood or plasma can be the difference between life and death. While dog tags are useful, Blockchain technology could be used to not only manage and securitize military or civilian data but, in a crisis, combat situation or terror attack, could rapidly allow medics to assess the people around them to help save lives. Blockchain-based medical records could reduce the costs of Department of Veterans Affairs administration data by up to fifty percent while allowing the military secure, lifetime access to their records, which only the patients themselves could delegate or allow access.

Refugee and International Detention Coalition (IDC) Management

Joanne Herring has one of the few success stories in Afghanistan, called the Herring Plan, where her policies allowed for successful development and protection of small cities. By creating a five-factor city development program in Khairabad, Afghanistan, Herring aided the refugee and border conflict infrastructure development. Adding a Blockchain based system would ease city growth and allow for the organized management of city infrastructure, people, systems, and payments.

Matthew "Griff" Griffin with Combat Flip Flops is another dramatic story. The continuing problem both faced with the inability to document displaced populations and refugees. Worse, displacement and separation allow for continual child soldier conscription and human trafficking issues (e.g. ISIS and Boko Haram). A Blockchain based identity solution could solve everything from identity management to the resettlement of people and return of assets following the cessation of a conflict.

Food Safety and Supply Chains

Poisoned food has killed thousands and is the tipping point of global food chain problems. As global weather changes, sea levels and inclement weather become larger concerns, safety and provenance of the food supply become more critical. Blockchains are poised to begin solving these challenges. [24]

Base/City/Opportunity Zone Management

The 2020s will see the development of Smart Cities and technology systems that will both deliver information and services while generating exponential quantities of data. Blockchain-based systems will allow for these data systems to work interchangeably and aid in economic development where data becomes the new oil. Additionally, moves by the NMTC to develop national (US) Blockchain standards will start driving new consensus, audit and identification technology by 2020.

Combatting Weaponized Internets

Russia is already planning an alternative Internet [25] while China is dabbling in its Internet infrastructure with a prediction that it will split by 2028. [26] Developing a Blockchain based Internet protocol tied to IPv6 or DNS or a new paradigm would easily allow us to combat digital foes that focus on manipulating information and access. Blockchain stacks like Prasaga will become newer models for data transport across networks on trillions of data connected devices.

Preparing for Future Risks – After ISIS and on to the "Laughing Man"

From Russian adversaries who have leveraged propaganda to accomplish everything from seeding discord in the Middle East to propaganda as news today, we have seen both risks and threats evolve. Today's terror threats of ISIS, AQIS (al-Qaeda in the Indian Subcontinent), Boko Haram, Al-Shabaab, and regional terror networks, funded by ISIS and al-Qaeda, will give way to evolving modes of terrorism once ISIS in Syria falls.

While insurgents can be killed – ISIS and Al-Qaeda's warped cult ideology resides online, in the dark web, and as PDFs and magazines that are passed among the disenfranchised in online forums. ISIS's focus on Europe in the past indicates that there is a risk of ISIS attacks across NATO countries. Recent ISIS suicide attacks on Iran's Revolutionary Guard and India's military have retrenched hostilities between the two and Pakistan, who in 2019, is still ill-equipped to tackle local insurgents, ISIS-linked terrorist groups, and emerging groups seeking regional hegemony.

Online bot and cyber-attacks are now beginning to see IoT compromises come to light. Couple this with the risks of Fitbits and App-connected devices and cellphones and there is a new need to understand that civilian hacking has entered the military realm. Social media is not only a threat to troops; it is a geo-taggable beacon that can share a secret base location on Instagram. Worse, researchers have been able to use simple tech and social media to misdirect NATO troops to ignore their orders. [27] Cryptocurrency and cyber-attacks have become synonymous while healthcare systems, including MRIs, are as susceptible to viruses and attacks if their systems are not secured or firewalled before they connect to a network.

Technical and critical system SOPs need to be reviewed and have quarterly refreshes, at a minimum, as the rate at which risks are changing accelerates every year. We are in an era when moving from defined and known enemies to amorphous groups (ISIS, ANTIFA, race supremacists) to individuals and smaller groups hidden by various online personas whose technology and cryptofinance knowledge makes them as dangerous as larger groups. We have begun to classify these latter groups and individuals as the "Laughing Man" or "Laughing Men" as their motivations tend to be a subset of a larger, more organized adversary.

These adversaries comprise the new range of international actors, domestic terrorists, and threats that technology, cryptocurrency, and changing digital and physical battlegrounds are beginning to produce. This landscape will also face rising challenges from Russia, China, Iran, North Korea, and regional African actors, none of whom will slow down their attacks if their propaganda machines have an impact. Instead, "Laughing Man" or "Laughing Men" will define the new ways in which we must develop our defenses. Lastly, consider the opportunities of the Blockchain and the opportunities for the US to think beyond how it operates today while tackling the challenges of tomorrow.

NOTES

1. https://doi.org/10.1177/1461444809105345.
2. https://yle.fi/uutiset/osasto/news/finnish_researcher_russia_ramping_up_its_information_war/8385245.
3. https://www.smh.com.au/world/finnish-journalists-jessikka-aros-inquiry-into-russian-trolls-stirs-up-a-hornets-nest-20160311-gng8rk.html.
4. https://www.dw.com/en/court-in-finland-finds-pro-kremlin-trolls-guilty-of-harassing-journalist/a-45944893.
5. https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.
6. Ibid.
7. https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.
8. https://www.washingtonpost.com/news/arts-and-entertainment/wp/2017/06/27/the-cnn-retraction-and-the-danger-of-relying-on-one-anonymous-source/?utm_term=.8a871f513283.
9. http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-worldwide-threat-assessment/.
10. https://propagandacritic.com/index.php/case-studies/isis-botnet/.
11. https://www.newsbtc.com/2018/08/10/researchers-identify-15000-strong-botnet-scamming-crypto-twitter/.
12. https://www.wired.com/story/creative-ddos-attacks-still-slip-past-defenses/.
13. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.
14. https://medium.com/@erin_gallagher/propaganda-botnets-on-social-media-5afd35e94725.
15. https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/daswani/daswani.pdf.
16. https://www.bbc.com/news/world-europe-47302938.
17. https://www.cyber.nj.gov/threat-profiles/botnet-variants/flusihoc?rq=china).
18. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#18c765b9425c.
19. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
20. https://www.ccn.com/breaking-major-crypto-brokerage-coinmama-hacked-450000-users-affected-in-massive-worldwide-breach.
21. https://smartereum.com/4791l/bitcoin-latest-update-argentina-accepts-payment-for-goods-sold-to-paraguay-in-bitcoin-btc-bitcoin-news-today-btc-usd-price-today/.
22. https://theish.us/wyoming-data-and-the-gold-rush-of-coming-crypto-regulations-4c3c06cd331d.
23. https://bitcoinexchangeguide.com/bitcoin-officially-classified-as-a-commodity-within-indonesias-borders/.
24. https://channels.theinnovationenterprise.com/articles/blockchain-set-to-solve-the-fake-food-problem.
25. https://www.dailymail.co.uk/sciencetech/article-5126931/Russia-plans-create-independent-internet-2018.html.
26. https://futurism.com/google-future-china-internet.
27. https://www.businessinsider.com/officials-tricked-nato-troops-into-disobeying-orders-with-social-media-20192.

The Cyber Defense Review

Research Articles

Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army

Lieutenant Colonel Christopher J. Heatherly
MSIV Cadet Ian Melendez

"In the future, the cyber threat will equal or even eclipse the terrorist threat."[1]
- Robert Mueller, 2013

ABSTRACT

Cyberspace represents a new domain of warfare unlike any other in military history. Cyberwarfare practitioners be they state actors, non-state actors or individual hackers, are capable of tremendous–and readily deniable–damage to an opponent's civil or military infrastructure. While recent events have focused upon the Islamic State's ability to use the Internet for recruiting purposes, the real danger to the West comes from its two primary competitors. The Russian and Chinese governments are suspected of using the entire spectrum of cyber warfare as both a standalone capability as well as effectively incorporating it into the more traditional domains of war. When faced by so many capable opponents, cyber training takes on an even greater criticality for U.S. Army officers. This paper focuses on a vital aspect of the U.S. Army's overall cyber ability by examining the training provided to Army officers beginning with their pre-commissioning education and continuing throughout their careers. It provides recommendations for improvements in officer education to ensure that future generations of American soldiers are prepared for the exigencies of cyberwarfare.

INTRODUCTION

The Greek philosopher Plato once said, "Only the dead have seen the end of war." While the truth of that statement is eternal, the way war is fought forever evolves. Just as the Japanese attack at Pearl Harbor on December 7th, 1941, signaled the end of the

Lieutenant Colonel Christopher J. Heatherly enlisted in the U.S. Army in 1994 and earned his commission via Officer Candidate School in 1997. He has held a variety of assignments in special operations, Special Forces, armored, and cavalry units. His operational experience includes deployments to Afghanistan, Iraq, South Korea, Kuwait, Mali, and Nigeria. He holds master's degrees from the University of Oklahoma and the School of Advanced Military Studies. Additionally, LTC Heatherly is a freelance author with 80+ published works.

battleship and Admiral Alfred Thayer Mahan's doctrine of decisive battle, cyberwar represents a new era and a new domain of combat. Cyberwar will not be fought by soldiers armed with rifles and machine guns, or by those inside tanks or jet aircraft. Nor will cyberwar have clear front lines separating opponents or even focusing exclusively upon an enemy's military capability. Cyberwar practitioners will employ the full spectrum of available cyber weapons against multiple civilian and military targets using a variety of military and non-military platforms. Bluntly stated, every U.S. Army soldier must be ready to fight on the digital battlefield.

Understanding the threat

The Islamic State's (ISIS) use of social media and the dark web to seduce young people across the globe and spread their message both at home and abroad are what most American soldiers are familiar with when it comes to the contemporary war in the cyber world. While not "hacking" in the traditional sense, ISIS' effective use of the cyber world as a recruiting tool cannot be ignored as an estimated 27,000 foreign fighters have traveled to Iraq and Syria since 2011.[2] Similar ISIS recruiting efforts have found, inspired or trained a growing number of "home grown" terrorists who have struck targets across Western Europe and the United States (US). ISIS' success does not stem from robust networks of data but rather the unlimited and largely unregulated nature of the World Wide Web. Twitter accounts, Facebook profiles, online podcasts, YouTube and other social media platforms all serve as effective, and often redundant recruiting tools. While these accounts are quickly shut down by a host of international policing agencies, they are just as rapidly and easily reestablished as they are readily accessible, inexpensive messaging platforms.

While ISIS and other terrorist groups effective social media strategies, the US' near-peer competitors,

Cadet Ian A. Melendez of Sammamish Washington developed a deep love for history and political science at an early age. After graduating from high school in 2012, he attended Bellevue College and was involved in the colleges Model United Nations program. Ian took part in many simulations at an international level and personally lead the institution to several high-profile Model UN conferences. Ian transferred to Washington State University (WSU) in January 2016 and joined the WSU Army Reserve Officer Training Corps (ROTC) detachment. Ian is the first cadet to lecture at the U.S. Army Command and General Staff College. He will graduate from WSU with a bachelor's degree in History and will earn Minors in Political Science and Military Science. Ian will receive his commission as a Second Lieutenant in the U.S. Army in May 2019. He will serve as a military intelligence officer while pursuing admission to a doctoral program in history.

China and Russia, present a more capable and dangerous cyberwar threat to the West. For the past 16 years, the US and its allies focused heavily on global counterterror operations with specific priority placed upon the Iraqi and Afghan theaters. During this same period, China and Russia developed, operated, and refined their own cyber capabilities. These nation states will employ, and indeed have already employed, both overt and covert means of cyberwarfare using a variety of military, paramilitary, third party, criminal organizations, and other proxies. Cyberwarfare incorporates many forms not all of which will entail a traditional offensive operation. Many cyber operations will instead focus upon information or intelligence gathering in preparation for or in concert with other traditional forms of attack.

The threat from China

China is a near peer competitor to the US already expanding its influence across the Asia-Pacific region with the long-term goal of becoming a global superpower. While not above using military force in pursuit of its objectives, the Chinese are masterful at employing cyber warfare against both military and commercial targets, particularly in information-gathering. To cite one high profile case, a Chinese national named Su Bin, spent several years hacking US defense contractors for data on the U.S. Air Force's newest fighter and transport aircraft. This information could be used to advance China's own aviation capabilities through reverse engineering or exploitation of perceived weaknesses in US aircraft. It should be noted that while the U.S. Department of Justice alleged Su worked in concert with China's government, specifically People's Liberation Army (PLA) Unit 61938, Beijing denied any involvement. [3] Following a lengthy investigation, in 2016 an American court sentenced Su to 46 months in prison and a fine of $10,000. Unfortunately, the damage was already done in that China

retained the information gathered in these attacks. Su's cybercrime was hardly unique and serves as evidence that the PLA has established dedicated units to act on the offensive in the cyber world. According to the New York Times, Unit 61398 is the source of several deliberate attacks by the PLA against the US military's cyber network. [4] A US National Intelligence Estimate, representing the analysis of all 16 US intelligence bodies, pointed to Chinese PLA officers or civilian contractors working at Unit 61938. [5]

While many of the details surrounding Unit 61938 are not fully known, such as its personnel composition, there is little doubt as to its past cyber activities and threat to Western interests. Unit 61398 is only one example of China's cyber playbook options. Author Joe McReynolds describes three different, but complimentary, approaches that Beijing employs against its competitors. These include operational military units, specialized civilian units and third party "external entities." [6] Additionally, a 2007 Foreign Policy article estimated China has 50,000 to 100,000 civilian hackers whose common interests bring them into occasional partnership with their nation's government. [7] Clearly, these groups represent a very real, highly skilled and robust danger to US national interests. A 2016 report from the US-China Economic and Security Review Commission bluntly stated, "among the most serious threats are China's efforts at cyber and human infiltration of US national security entities." [8]

The threat from Russia

Another primary US competitor, the resurgent Russian government, is widely believed to utilize similar tactics in its own cyber arsenal. According to a 2017 *Christian Science Monitor* article, the Russian government uses criminal computer hackers as proxies against targets in the West. This tactic provides two tremendous benefits: it ensures Moscow retains access (and control) over some of the most capable cyber operators and gives the Russians plausible deniability against Western reprisals. [9]

The successful employment of cyber warfare, either as a standalone capability or in conjunction with other systems, is nothing new to the Russian government. Indeed, the Russians employed cyber in support of conventional attacks during their 2008 invasion of Georgia–a first in military history. In that engagement, Russia allegedly overwhelmed Georgia's internet and computer infrastructure limiting Tbilisi's ability to coordinate its defense. [10] No doubt their capabilities have improved and perhaps been further refined in other operations over the past 9 years.

Like China, Russian cyber operations also target non-military entities as evidenced by the 2010 "cyberbomb" discovered in the NASDAQ exchange. [11] A near successful attempt at what could have been the largest data leak in the history of the US stock market caused many corporations and investors to seriously question the security of both their data and personal information, as well as the legitimacy of the market itself. [12] During the subsequent investigation, the National Security Agency (NSA) successfully traced the attack

back to several Russian citizens including one Aleksandr Kalinin of St. Petersburg, Russia. Kalinin had previously stolen millions of credit card numbers and placed malware on major American corporations like Dow Jones, 7-Eleven, JetBlue, and JC Penny. [13] US federal prosecutors charged Kalinin and his co-conspirators with the attack although he has thus far avoided prosecution. [14] According to a report on Business Insider, "the NSA recognized the malware from a previous version, built by Russia's main spy agency. However, this time it was much more dangerous–it had the ability to disrupt the entire network, potentially wiping out Nasdaq altogether." [15] The Russian methodology of employing hackers, in lieu of sending them to prison, incentivizes their cooperation and affords Moscow a rather unique means of recruitment unavailable, or at least unpursued, to other nations. [16]

Additional reports warn of Russian attempts to hack into the US electric power grid and natural gas pipelines. [17] The impact of these attacks cannot be overstated as they would cause mass power outages or damage the physical infrastructure itself. The threat of and resultant damage from cyber security failures continues to be of national significance with many more high-profile attacks making headlines.

Current U.S. Army Cyber capability and training

The US military has its own cyber units, education and training, although for the purposes of this paper, we will primarily focus upon the Army. The first Army unit formally stood up for this new brand of warfare was the U.S. Army Cyber Warfare Command which was founded in 2010. The Army later designated this unit as an Army Service Component Command in 2016, authorizing it to "gather resources to organize, develop, and employ cyber capabilities in support of the Joint Force." [18] During testimony before a Subcommittee of the Senate Armed Services Committee (SASC) on emerging threats and capabilities in 2015, then ARCYBER Commanding General LTG Edward Cardon said, "After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills." [19] LTG Cardon further stated the Army would have 41 Cyber Mission Force team, working for the global combatant commanders, in the active component with an additional 21 Cyber Protection Teams in the National Guard or Army Reserves by the end of Fiscal Year 2016. [20] To effectively meet the threats on the cyber battlefield, the Army projects it will need an additional 355 officers, 205 warrant officers and 700 enlisted soldiers in the ranks. This number, combined with the planned 3,000 civilian contractors, will provide the Army with a more robust force both in terms of size and domain knowledge. [21] Recognizing the need for cyber leaders, the Army began commissioning new lieutenants directly into the newly created Cyber Branch. The Army has also issued calls for branch transfers to Cyber Branch of more senior officers, up to the rank of colonel, who already possess the skills, education and training required to meet the demands in this field.

For the bulk of the Army's non-cyber branch personnel–in other words the rank and file soldiers, non-commissioned officers and officers in the Active Duty, National Guard and

U.S. Army Reserve components–cyber training consists of the online "Cyber Awareness Challenge." Taken annually, the Cyber Awareness Challenge is presented in a chapter format with the goal of "providing enhanced guidance for online conduct and proper use of information technology by DoD personnel, simulates the decisions that Federal government information system users make every day as they perform their work." [22] Test takers are awarded notional digital trophies for properly answering questions posed in a set of scenarios involving common work-related tasks. Although described as "first-person simulations and mini-games that allow the user to practice and review cybersecurity concepts in an interactive manner," the actual training received is limited in scope and value to leaders. [23] However, the Cyber Awareness Challenge provides no information on more advanced enemy cyber capabilities, nor US offensive or defensive cyber capabilities leaders will need in future operations.

Future Army officers enrolled in the Army Reserve Officer Training Corps (ROTC) receive some cyber instruction during their two to four years of military science education prior to earning their commission as lieutenants. There are 275 primary Army ROTC programs at universities and colleges across the US that train approximately 30,000 cadets and commission over 5,000 new officers per year. For most college students, ROTC is also their first encounter with the unique demands of military life and the formative experience beginning their careers as commissioned Army officers. As such, it is the largest source of new Army officers and should be, and indeed must be, the formative step in cyberwarfare training. In addition to taking the same Cyber Awareness Challenge, ROTC cadets also receive one class describing the new cyber branch career field. The authors see this as a prime opportunity to shape the future cyber ability of the force well in advance of their actual entry into military service.

Upon commissioning from ROTC, new lieutenants attend further schooling at a Basic Officer Leader Course (BOLC) based upon their respective branch, i.e., Armor, Military Intelligence, etc. While individual BOLC schools provide specialized training pertinent to their chosen fields they all share a common core of education required for any commissioned officer. The authors spoke with several new officers attending BOLC while researching this paper and found none of them had received any cyber training beyond the Cyber Awareness Challenge. This deficit is a glaring gap in officer education given these soldiers will serve as the Army's leadership for the next thirty or more years into the future. Failure to institute an appreciation for operational advantages and dangers of cyberwarfare now will create challenges in cyber application throughout the entirety of their service careers.

Examination of another level of the officer education system (OES) reveals the same problem exists at other levels. The top half of the Army officer corps are centrally selected to attend the Command and General Staff College (CGSC), sometimes called Intermediate Level Education (ILE), usually in their eight to tenth year of military service. This course

is approximately ten months in length for those who attend the resident version. CGSC, located at Fort Leavenworth, Kansas, has made some inroads to improving cyber to address the very real threat its graduates will face as they return to the operational force.

Currently, the core curriculum provided to all CGSC students includes a two-hour block on cyberspace with additional cyber instruction as part of the lessons on Command and Control and Fires Integration. Additionally, CGSC includes some cyber play in the various student war game exercises conducted at the end of each major block of instruction. American officers attending CGSC have the option to take a classified cyber elective although class attendance is limited by security clearance requirements and instructor availability. This class, which is double the length of a normal CGSC elective course, includes a mix of classroom instruction, guest speakers and practical exercises. [24] While this nascent initiative is to be applauded, waiting until the midpoint of a military career comes too late for maximum benefit.

The CGSC's approach to cyber education further highlights some of the challenges facing the Army's Training and Doctrine Command (TRADOC) which is responsible for soldier education. First, the pool of available cyber instructors is limited to those with the proper security clearance, education and experience. The CGSC faculty team, for example, is largely made up of civilian instructors who retired from active military service before cyber warfare was a standard consideration. No doubt the instructors are dedicated to their profession and the education of their students, but they will require additional training to bring cyber relevance to the classroom. The pace of change in cyber warfare is rapid and will also require the military's educational platform to quickly develop both courses and instructors. Nor is cyber training a "once and done" type of learning but instead requires dedicated study over a career. The classification of the material itself presents a third challenge. Knowledge of and access to US cyber capabilities must be limited to those with a verified need to know lest it fall into the hands of US competitors.

Improving Army Cyber readiness

We suggest several actions for the U.S. Army to consider improving its current cyber capabilities and training. First, the Army must promote the seriousness of the threat to the entire force and not place the burden to dominate this new domain of warfare on cyber missioned units. The U.S. Marine Corps has a mindset that every Marine is a rifleman first. Given that every Soldier has access to personal and government IT systems, smart phones and the like, the Army must adopt the same mind frame but expand it to include every soldier is a cyber warrior as well.

This new mindset must begin the moment a civilian recruit steps forward and volunteers to serve. The Army must adopt an aggressive national cyber recruiting strategy targeting those citizens with the skill sets demanded by the branch. Similarly, local Army recruiters must identify qualified applicants for cyber branch positions and explain the unique as-

pects of this military occupational specialty (MOS). A suggestion, not without controversy, is to redirect personnel who are not physically qualified into civilian cyber opportunities that do not have the same operational demands as uniformed soldiers. This would require Army recruiters to place civilian applicants but would also contribute to the Army's overall ability to hire new personnel. Reducing or eliminating the physical requirements for uniformed personnel or the criminal, educational or moral requirements for any Army applicant is categorically rejected by this paper. The Army must further press for more efficient hiring procedures to bring on the required personnel now. During his Senate hearing, LTG Cardon relayed the challenges of hiring personnel "given internal federal employment constraints regarding compensation and a comparatively slow hiring process." [25]

Beginning with their initial training and continuing throughout the entirety of their careers, soldiers must be routinely educated on cyber threats in "hands on classes" taught by experts who are able to demonstrate the dangers of cyber warfare. Instruction should be multifaceted across the entire spectrum of threats including improper use of email, social media accounts, personal cell phones or computers as well as the potential damage of cyberattack during the conduct of actual military operations. Examples of such effective training would include case studies based on real soldier cyber incidents, ruthlessly enforcing operational security (OPSEC) in both garrison duties and field exercises, classes on security classification regulations and drastically reducing the prevalence of personal computing or communication devices at home station or deployed locations.

Additionally, the Army must continue to offer incentives to retain the best cyber personnel in the formation lest we lose them to opportunities elsewhere in the civilian cyber fields. The introduction of competitive bonuses for reenlisting cyber soldiers like those offered to the special operations is but one possible solution. While some special forces bonuses top $150K, the financial and time resources of recruiting and training new cyber personnel would be much greater. [26] Instituting educational partnerships, exchanges or simply sending cyber personnel to undergraduate, graduate or doctoral programs is another method to train and retain the best personnel.

The Army should seek outside expertise and solutions by partnering with industry and educational institutions also combating cyber threats. While hardened infrastructure and new cyber defense technologies will afford some measure of defense against future attacks, these are not sufficiently robust or effective to ignore the human component required to meet the threat. A 2017 Real Clear Defense article neatly sums up this problem stating, "Promising technologies like artificial intelligence — software that autonomously detects and thwarts attacks — are fueling investment and innovation but should not be seen as silver bullets." [27] Simply investing money and energy in the existing paradigms as the quote would suggest is not enough to remedy the situation and put the military on par or beyond that of US near-peer adversaries. Utilizing and working alongside existing academic

structures brings in a new non-military perspective from citizens who are in many ways the experts of the cyber field. The University of Dallas, for example, offers undergraduate, graduate, and post-graduate degrees in the various subfields of cyber. A Master of Science in Cyber Security from the University of Dallas teaches students a litany of skills including methods of data protection, legal issues and protections under the law, network security and digital forensics. Proving the connection between cyberattacks and instigator is incredibly difficult and one of the most attractive features of cyberwarfare. Increasing the number of experienced soldiers and civilian contractors armed with the educational background and experience on tracing digital evidence could provide the definitive evidence required for the US to defend against or respond appropriately to future cyberattacks.

More pragmatically, leaders must enforce proper communication procedures and cyber OPSEC in all aspects of a unit's daily duties whether in garrison or in the field. Commanders must hold Soldiers accountable, and they themselves must be held accountable, for violations of standing cyber regulations, rules and laws that threaten the readiness or operational security of their units. Leaders stating, "it's too hard" or "I am assuming risk" and willfully ignoring cyber OPSEC will lead to US casualties or even defeat in warfare against peer or near-peer opponents.

It is equally important the Army continually fund both cyber units and cyber training to ensure all soldiers are prepared for cyber warfare. During the Global War on Terrorism, the Army stood up or expanded numerous capabilities such as counter IED, working dogs, military transition teams (MITT) or agricultural development teams (ADT) to support combat units lacking these enablers in their organic formations. Many of these same enablers were reduced as the Iraq and Afghan theaters drew down. Attempts to expand these programs will long stand up times in any future conflict. Additionally, the Army often failed to promote or select for higher command the personnel assigned to these units, particularly those officers commanding MITTs, all but ensuring the "best and brightest" would seek assignment elsewhere. We cannot afford to make the same mistakes with cyberwarfare.

CONCLUSION

Famed American humorist Mark Twain observed, "history doesn't repeat itself, but it does rhyme." [28] America will go to war again. The cyber domain will play a prominent, if not decisive, role in that war. The only questions which remain unanswered are the opponent, location, and timing of that future conflict. Potential enemies, namely China and Russia, have already shown a willingness and ability to incorporate cyber into their offensive and defensive strategies. The Army must be ready – through education, training and partnership with industry leaders – now to fight and win on the cyber battlefield. This readiness will be found in the education of the next generation of Army leaders.

NOTES

1. Federal Bureau of Investigation, RSA Cyber Security Conference remarks, https://archives.fbi.gov/archives/news/speeches/working-together-to-defeat-cyber-threats.
2. *The Daily Telegraph*, Iraq and Syria: How many foreign fighters are fighting for ISIL?, http://www.telegraph.co.uk/news/2016/03/29/iraq-and-syria-how-many-foreign-fighters-are-fighting-for-isil/.
3. *The Washington Post*, Businessman admits heling Chinese military hackers target U.S. contractors, https://www.washingtonpost.com/world/national-security/businessman-admits-helping-chinese-military-hackers-target-us-contractors/2016/03/23/3e74e4a4-f136-11e5-85a6-2132cf446d0a_story.html?utm_term=.106972b16120.
4. *The New York Times*, Chinese Army Unit Is Seen as Tied to Hacking Against U.S, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?emc=na&_r=1&.
5. Ibid.
6. *The Daily Beast*, China Reveals Its Cyberwar Secrets, http://www.thedailybeast.com/china-reveals-its-cyberwar-secrets.
7. *Foreign Policy*, China's Hacker Army, https://foreignpolicy.com/2010/03/03/chinas-hacker-army/.
8. *The Washington Free Beacon*, Report: Chinese Spies Stole Pentagon Secrets, http://freebeacon.com/national-security/report-chinese-spies-stole-pentagon-secrets/.
9. *The Christian Science Monitor*, How Russia and others use cybercriminals as proxies, https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies.
10. *The New York Times*, Before the Gunfire, Cyberattacks, http://www.nytimes.com/2008/08/13/technology/13cyber.html.
11. *Business Insider*, The Massive Hack of the Nasdaq That Has Wall Street Terrified of Cyber Attacks, http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7.
12. CNN, Russian hackers placed 'digital bomb' in Nasdaq – report, http://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/index.html.
13. The United States Department of Justice, Russian National Charged in Largest Known Data Breach Prosecution Extradited to United States, https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states.
14. NJ Advance Media, Russian hackers plead guilty in N.J. in worldwide $300M credit card scheme, http://www.nj.com/news/index.ssf/2015/09/russian_hackers_plead_guilty_in_nj_in_worldwide_30.html.
15. *Business Insider*, The Massive Hack of the Nasdaq That Has Wall Street Terrified of Cyber Attacks, http://www.businessinsider.com/nasdaq-attacked-by-hackers-2014-7?IR=T.
16. NJ Advance Media, Russian hackers plead guilty in N.J. in worldwide $300M credit card scheme, http://www.nj.com/news/index.ssf/2015/09/russian_hackers_plead_guilty_in_nj_in_worldwide_30.html.
17. CNN, Russia attacks U.S. oil and gas companies in massive hack, http://money.cnn.com/2014/07/02/technology/security/russian-hackers/index.html.
18. The United States Army, Army Announces ARCYBER as an ASCC, https://www.army.mil/article/171513/army_announces_arcyber_as_an_ascc.
19. The United States Army, Army may create cyber career field for civilians, https://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/.
20. Ibid.

NOTES

21. The Army Times, Staffing goal for Cyber branch totals nearly 1,300 officers, enlisted soldiers, http://www.armytimes.com/news/your-army/2015/06/15/staffing-goal-for-cyber-branch-totals-nearly-1300-officers-enlisted-soldiers.
22. The Center for Development of Security Excellence, CyberAwareness Challenge 2019 for Department of Defense (DoD) DS-IA106.06, http://www.cdse.edu/catalog/elearning/DS-IA106.html.
23. Ibid.
24. Kurt Vandersteen, email to author, August 8, 2017.
25. The United States Army, Army may create cyber career field for civilians, https://www.army.mil/article/146485/Army_may_create_cyber_career_field_for_civilians/.
26. *The Stars and Stripes*, $150,000 bonus offered for some Special Forces, https://www.stripes.com/news/150-000-bonus-offered-for-some-special-forces-1.75636#.Wa0oEbpuLIU.
27. *Real Clear Defense*, Will U.S. Cyberwarriors Be Ready for the Next Big Hack?, http://www.realcleardefense.com/articles/2017/08/17/will_us_cyberwarriors_be_ready_for_the_next_big_hack_112066.html.
28. Good Reads, Mark Twain Quotes, https://www.goodreads.com/quotes/5382-history-doesn-t-repeat-itself-but-it-does-rhyme.

The Concept of a "Campaign of Experimentation" for Cyber Operations

Dr. Robert R. Hoffman

ABSTRACT

A Campaign of Experimentation is necessary for the United States to achieve a robust capability in cyber defensive and offensive operations, that is effectively and efficiently integrated with operations in cyber-kinetic domains. The article describes challenges for such a Campaign, regarding experimental design, logistics, measurement, and methodology.

The campaign concept

In a report titled "Code of Best Practice: Experimentation," David Alberts and Richard Hayes [1] asserted:

> Experimentation is the lynch pin in the DoD's strategy for transformation. Without a properly focused, well-balanced, rigorously designed, and expertly conducted program of experimentation, the DoD will not be able to take full advantage of the opportunities that Information Age concepts and technologies offer.

Alberts and Hayes continue to explain why the DoD needs to conduct "Campaigns of Experimentation." First, no single experiment improves knowledge enough to support a major goal such as transformation. Individual experiments can only look at a limited number of variables and contexts, and therefore must be integrated with other experiments to ensure that limiting conditions are properly understood. Series of experiments are needed to differentiate between competing hypotheses to yield actionable knowledge. Second, individual experiments within a series are likely to generate some unexpected findings that are both important and interesting. Experimentation campaigns provide the opportunity to explore those novel insights and findings, as well as their implications. These ideas are all fundamental to the methodology that has been established in the field of experimental psychology. [2]

Robert R. Hoffman received his Ph.D. in experimental psychology from the University of Cincinnati. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a Fellow of the Association for Psychological Science, a Fellow of the Human Factors and Ergonomics Society, a Senior Member of the Association for the Advancement of Artificial Intelligence, and a Fulbright Scholar. He has been recognized internationally for his research on the psychology of expertise, the methodology of cognitive task analysis, and the issues for the design of complex cognitive work systems, including cyber work systems.

We are now in what Alberts and Hayes referred to as the "Information Age Transformation". [3] While the scientific rationale for a Campaign of Experimentation is based on the above considerations, the practical rationale is equally significant. The current world situation is one in which adversarial relations and conflicts are characterized by extreme levels of uncertainty, complexity, fast pace, and dynamics. The delivery of a technology or weapon system is not the end of a procurement. It is the beginning of a phase in which operations and experimentation must be tightly coupled. What this means is that the traditional separation of experimentation and operations must not just be blurred but dissolved. As ever-more complex automation is injected into the workplace, the work must be continuously observable.

What makes cyber operations unique

The domain of cyber operations is unique in several respects, which further justifies the application of the Campaign concept. Though network operations is not a new type of work, the work of U.S. Cyber Command (USCYBERCOM) Cyber Protection Teams (CPTs) is relatively new. While there are many experts who have considerable experience in network operations, many of them work in the private sector. For CPT certification and performance evaluation there remains a gap in our ability to appropriately describe the work in terms of proficiency scaling and learning curves. It is not enough to say that an individual has specific qualifications as evaluated by a checklist method. One needs a full and rich description of what it means for an individual to be an apprentice, journeyman, expert or master. We know this to be true for all other complex sociotechnical domains. [4]

Cognitive work in the cyber domain is a moving target as it involves an adaptive and deceptive adversary and a rapid pace of technological change. The pace of change in the work and the technology far outstrips the speed at which standard controlled experimentation can be conducted. As both cyber work and cyber tools continue to evolve and cyber Concepts of Operations (CONOPS) continue to adapt, there is the need to understand the issues and provide recommendations to ensure an effective cyber force. Mission types will change as threats and adversaries themselves change and adapt. Research must be ongoing.

Cognitive work is messy. Numerous uncontrollable variables come into play and can influence logistical and operational activities. Were experimentation to be conducted in the traditional manner of isolation and control of variables, the research would not represent the actual work ecology. Tasks that are tightly bound by procedure when conducted in the laboratory might permit careful measurement, but can also distance the task process from real world variables. Thus, research is needed that combines both laboratory and field experimentation.

There are more variables that play a crucial role than can be controlled and manipulated in any single experiment: the experience level of the cyber workers who are research participants, the technologies utilized, the different sorts of missions, and the various logistical demands that must be met. Research designs can adopt any of several options, ranging from single, simple experiments that evaluate baseline performance, to larger, more complex designs that involve the manipulation of more than one variable. There must be an on-going process of developing useful experimental designs and mapping them on to the immediate needs that emerge.

There is no clear or straight path from high-level concepts such as “efficiency” and “quality” to operationally defined measures that are useful in experimentation and evaluation. Cyber operations involve multiple sub-tasks. The tasks and sub-tasks are not strictly linear or stepwise but are often conducted in parallel. [5] These and other features of cognitive work mean that experimentation is necessary to develop and refine appropriate measures and metrics.

Concepts for experimentation on cyber work processes and tools challenge our fundamental notions of statistical testing and analysis. A primary reason is sample size due to resource limitations. Suppose, for example, that one has a new software tool suite to evaluate. The evaluation must involve multiple cyber operators attempting to learn and use the new software tools, but multiple cyber operators are often not available. And when they are, they must be selected for having similar levels of experience, which means that experimental designs based on traditional parametric statistical significance testing can be insufficient. Therefore, methods of order statistics and concepts of practical significance must be considered. It should be noted that a Campaign of Experimentation represents a unique and important opportunity to advance our scientific methodology for statistical analysis of studies having small sample size, and for the large-scale experimentation that is resource

constrained. In addition to mandating advances on the concept of practical significance, it is necessary to make advances on the estimation of effect sizes given small sample sizes. [6][7]

The above considerations all mandate a Campaign of Experimentation as an on-going process. The Campaign would be conducted not only to address the above needs but to also recognize a fundamental fact of scientific experimentation: that the purpose of experimentation is to continually improve and refine the experimental and measurement methods.

A Campaign of Experimentation is necessary to inform cyber CONOPs. Research evaluates the technologies and software systems for their understandability, usefulness, and usability. The performance of cyber operators must be empirically observed and evaluated to ensure that the work is effective and is of the highest quality. Research shapes our understanding of proficiency levels for selection and training.

Moving from the campaign concept to a cyber-specific methodology

Alberts and Hayes [3] presented some "barriers to transformational campaigns." For instance, they cautioned against the imposition of unrealistic schedules on experimentation, the failure to utilize an extensive and rich set of realistic scenarios, and the failure to adequately fund the experimentation. While expressing such important cautionary tales, the work of Alberts and Hayes did not delve deeply into the procedural and methodological details involved in experiments of the sort being envisioned, specifically experimentation on Cyber Operations.

However, results from recent research activities at the Cyber Immersion Laboratory of USCY-BERCOM have illuminated several vital principles that take the broad Alberts-Hayes concepts and apply them specifically to Cyber Operations. The NetMap activity [8] and the Deployable Mission Support System (DMSS) activity [9] engaged CPTs in processes of network mapping and vulnerability analysis. The purpose of these activities was to observe and evaluate the performance and workflows of CPTs, observe and evaluate the usability and usefulness of the available software support systems and tools, and initiate a process of capturing the knowledge and reasoning strategies of the most experienced CPT members. These activities required the establishment of a virtual cyber environment, the scripting of various scenarios, the coordination of multiple CPTs, and other logistical elements required for large-scale experimentation.

The process of designing, implementing and conducting these activities revealed many challenges. For example, it was determined that each CPT member would have to complete a demographic survey, complete various checklists as they accomplished sub-task goals, complete a post-event questionnaire, among other tasks that are not a part of regular CPT activities. Once the requisite materials were fleshed out and used, it became clear that the participants were in some sense being over-burdened. Clearly, the experimental context should not demotivate the participants. Several additional challenges emerged from these projects.

Experiment design challenges

Experiments require that some variables are controlled while some are manipulated. The manipulated variables are the ones whose causal impact is of immediate interest. The controlled variables are the ones that are known or believed to have an impact, but that must be held constant for the assessment of the manipulated variables. For instance, one might want to conduct an evaluation of a software tool but hold participant experience level constant by involving only the highly experienced CPTs (a control variable). One might want to have CPTs work on more than one type of attack (a manipulated variable) to evaluate task difficulty.

There are more important variables that can be manipulated and controlled than can be logistically incorporated. Take the example of task difficulty. A CPT conducts a task (e.g. vulnerability analysis) using software Tool A and then repeats the task using Tool B. But in using tool A the first time, the CPT will have become familiar with the network under study, perhaps making it only seem as if they perform better on the second task. This means one needs a counterbalanced order, in which one CPT uses Tool A first and the other CPT uses Tool B first. The alternative is to build more than one test network. Then, there is the matter of CPT experience. Do we want to make decisions about tool usability based on the performance of trainee CPTs or based on the performance of experienced CPTs? However, one approaches the design challenge, the experiment design can quickly become complicated.

Another design challenge is that the findings from a highly controlled environment might not apply in messy real-world instances where the work involves many uncontrolled and uncontrollable variables. If one wants to know about such things as CPT performance or tool usability, then those things must be evaluated in ecologically valid and varied conditions rather than in tightly controlled environments in which key variables get frozen out. Experiments must let the nasty variability of the world enter the picture. This runs counter to the traditional paradigm of laboratory experimentation. It is therefore crucial for a Campaign to involve specialists who have had experience in laboratory experimentation, and who can take point on matters of experimental design and measurement.

Logistic challenges

The challenges of experimental design mentioned above spill over to logistics. A counterbalanced design involving, for example, high and low experience CPTs, multiple software tools, and the need for multiple test networks, etc., means mustering human and machine resources that can be hard to come by. That nasty variability of the real world can entrain considerable logistical problems. For example, even simple things (such as failure of a disc to initialize) can completely shut down a large-scale experiment and send 50 people home. Just as unexpected things happen in the "real world," unexpected things happen in the context of large-scale experiments. This is something that the researchers must navigate.

Measurement challenges

There is a tendency for researchers to seek easy, automation-based methods for collecting data. In the case of cyberwork, for instance, this might involve examining logs of operator actions. But log data do not inform you about what the operator was thinking, anticipating, or worried about. Logs would tell you something about what they were doing, but not why they were doing it. Another measure that is often mentioned is eye movements. Eye movements may tell you what an operator is looking at, but they do not always tell you what the operator is thinking or is worried about.

There is a distinction between objective and subjective data, coupled with the mistaken belief that subjective data do not make for genuine science. It has been argued in the philosophy of science for decades that the distinction between objective and subjective data is mythical; all measures have both subjective and objective aspects to them. [10] Cyberwork is deeply and necessarily cognitive. The analysis of CPT members' reasoning and knowledge is central to the development of an effective workforce and can only be evaluated if the researches somehow "get inside the heads" of the CPT members, primarily by asking questions in structured cognitive interviews. [11] The most important data always come from the participants' answers to probing questions. What are you thinking? What are you anticipating? What are you worried about? What is your machine doing?

The drive to find useful metrics brings in another measurement challenge. Certainly, meaningful measures are needed, including measures that can be taken automatically, but this is not the same as metrics. A metric is a decision point, a value on some measurement scale that informs decision making. Is a score of 70% correct indicative of good performance, or poor performance? Well, it depends on the task. Metrics do not derive directly, easily, or automatically from measures. Theories provide measurable concepts, and measures are recipes for taking measurements, but metrics come from policy. [12]

The drive to automate measurement, and the belief that automated measures are objective, combined with the belief that all scientific and policy answers can be found if only if one has good metrics are all beliefs that blind researchers to the fact that research is difficult.

Methodological challenges

It is important to keep in mind one of the purposes of experimentation and measurement is to continuously adapt and improve the experimental and measurement methodologies, especially in the Campaign context where events provide opportunities that could be easily missed. For instance, there may be a lull in the cyberwork activity (for any of a variety of reasons). From a research perspective, lulls are an opportunity to conduct cognitive interviews with the CPT members to assess such things as their training and development of expertise, to elicit information about their reasoning strategies, and the experience that enabled them to achieve expertise. They can be asked about how they learn the differences

between their actual work process and doctrine (i.e. lessons learned and best practices), the tool functionalities and capabilities that they need or desire. [13]

Based on experience in the NetMap and DMSS projects, recommendations can be offered concerning methodology. First, it is recommended that a Dry Run study be conducted before the actual experiment activity. In a Dry Run, the researchers themselves serve as cyber operators and attempt to conduct the tasks, using a highly scripted workflow. The purpose is to evaluate the planned experiment procedure and familiarize the researchers with the workflow.

The second activity is a Pilot Study. A select, highly-experienced CPT conducts the experiment procedure while researchers observe and present probe questions. The purpose is to evaluate the planned experiment procedure and familiarize the researchers with the workflow, but also to forge an all-important performance baseline.

Third, experiments need to have a Conductor, a selected researcher who issues directions to observers and CPT operators, starting in the scripted dry run and continuing in the pilot study. The Conductor keeps things coordinated and gains an appreciation of where the planned experiment procedure falls on the continua of complexity and ecological validity. Experiments of the sort that have been referenced in this article involve upwards of six researcher/observers, five CPTs, and additional support and technical staff.

Fourth, there must be a deliberate effort to build a useful baseline, which would start with the Pilot Study and continue through to the Baseline Study, in which a select, highly experienced CPT engages in the experimental procedure and tasks without any direction, scripting, or interference from the researchers. The purpose will be to evaluate the ecological validity of the scripted workflow and procedure and refine the performance baseline and other measures.

CONCLUSION

The need to develop a U.S. Government Cyber CONOPs and capability based on the Alberts-Hayes concept of a Campaign of Experimentation is apparent. It is in some respects being implemented in current studies at facilities such as the Cyber Immersion Lab of USCYBERCOM and the U.S. Army's Cyber Human Integrated Modeling and Experimentation Range. To some extent, the Campaign concept is being partially implemented in various cyber events, exercises, and competitions. The purpose of this article is to motivate a programmatic process for fleshing out and fully implementing the Campaign concept with specific reference to the unique needs and challenges of cyber work. A broader implication of the challenges presented here is that the full implementation of the Campaign would require the coordinated integration of resources and activities across several branches of government, including but not limited to the Department of Defense.

Another challenge that should be noted involves both logistics and experimentation. Since a Campaign can span years, and the individual experiments can span months in planning and implementation, it is crucial for there to be continuity of the Campaign leadership. A stable vision accompanied by a deep understanding of the Campaign and its individual projects and experiments will be necessary for Campaign success.

DISCLAIMER

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

NOTES

1. D.S. Alberts and R.E. Hayes, (2002), "Code of Best Practice: Experimentation." Command and Control Research Program, Department of Defense, Washington DC, xi.
2. B.J. Underwood, (1966), Experimental psychology. New York: Appleton-Century-Crofts.
3. D.S. Alberts and R.E. Hayes, (2006), "Code of Best Practice: Pathways to Innovation and Transformation." Command and Control Research Program, Department of Defense, Washington D.C., 136-139.
4. R.R. Hoffman, P. Ward, L. DiBello, P.J. Feltovich, S.M. Fiore, and D. Andrews, (2014), Accelerated Expertise: Training for High Proficiency in a Complex World. Boca Raton, FL: Taylor and Francis/CRC Press.
5. S. Trent, R.R. Hoffman, D. Merritt, and S. Smith, (in press), Modeling the cognitive work of cyber protection teams. The Cyber Defense Review.
6. R.R. Hoffman, P.A. Hancock, and J.M. Bradshaw, (2010, November/December), Metrics, metrics, metrics, Part 2: Universal Metrics? IEEE Intelligent Systems, 93-97.
7. R.R. Hoffman, M. Marx, R. Amin, and P. McDermott, (2010), Measurement for evaluating the learnability and resilience of methods of cognitive work, Theoretical Issues in Ergonomic Science. Published online at iFirst, DOI: 10.1080/14639220903386757.
8. S. Trent, R.R. Hoffman, and S. Lathrop (May 2016), Applied Research in Support of Cyberspace Operations: Difficult, but Critical, The Cyber Defense Review, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136076/applied-research-in-support-of-cyberspace-operations-difficult-but-critical/.
9. S. Barna, (with 9 others) (2017), "Deployable Mission Support System Assessment." AOS Report No. AOS-17-0524, Applied Physics Laboratory, Johns Hopkins University, Laurel, MD.
10. F.A. Muckler, (1992), Selecting performance measures: "Objective" versus "subjective" measurement. Human Factors, 34, 441-455.
11. B. Crandall, G. Klein, and R.R. Hoffman, (2006), Working Minds: A Practitioner's Guide to Cognitive Task Analysis. Cambridge, MA: MIT Press.
12. R.R. Hoffman, (2010), Theory → Concepts Measures, but Policies → Metrics. In E. Patterson and J. Miller (Eds.), Macrocognition metrics and scenarios: Design and evaluation for real-world teams, London: Ashgate, 3-10.
13. R.R. Hoffman and M.J. McCloskey, (2013, July/August), Envisioning Desirements, IEEE Intelligent Systems, 82-89.

Seeing is Believing: Quantifying and Visualizing Offensive Cyber Operations Risk

Major Michael Klipstein, Ph.D.

ABSTRACT

This paper presents an integration of decision-maker preferences, quantitative risk analysis, and simulation modeling to aid commanders in choosing a course of action (COA) for conducting offensive cyber operations (OCO). It incorporates information from subject matter experts (SMEs) to parameterize a simulation model which provides decision support to mission planners when evaluating different COAs. The methodology is exercised and evaluated by cyberwarfare practitioners. The research findings demonstrate its value for increasing the ability of inexperienced personnel to make COA selections on par with experienced personnel, providing greater perceived understanding of risk defined as meeting the constraints of both cost and effectiveness, mitigating confusion or ambiguity resulting from subjective terms, and providing greater consensus of COA selection among practitioners in the aggregate. The advantages of this approach are significant as it produces a portrait of each COA that reveals the effect of the uncertainties that the SMEs admit pertaining to each of their outcome estimates. Given the value functions and trade-off weights of the commander, these translate into a meaningful portrayal of the risk to the decision maker in each COA.

INTRODUCTION

Military commanders and their staff below the national command level are ill-prepared to assess risks for conducting offensive cyber operations (OCO) (Department of Defense, 2017a, Department of Defense, 2017b). The man-made cyber domain exhibits four unique traits that differentiate itself from the traditional military domains. First, a lack of permanence exists for objects within the domain as they appear, disappear, or change at rapid speed. Next, the domain lacks measures of effectiveness for operations. The view of the virtualized battlefield is limited, and an accurate feedback loop for actions and

MAJ Michael Klipstein, Ph.D. has been involved with cyberspace operations since his 2010 assignment to USCYBERCOM. Following this, Michael worked for two years in Tailored Access Operations (TAO) as part of the National Security Agency (NSA). Michael then led the Army's National Mission Team; the offensive cyber team tasked to conduct operations to protect the critical infrastructure and key resources of the nation and to answer intelligence requirements as assigned by the President. Following success with the NSA, he created and trained two national level cyber protection teams charged with protecting the DoD's networks from nation-state actors. In 2014, Michael attended the Naval Postgraduate School in California to attain his Ph.D. in Information Sciences. Currently, Dr. Klipstein is assigned as a senior research scientist and the Chief of Outreach at the Army Cyber Institute at West Point. He assists the Joint Staff and ARCYBER with research problems facing the international cyber community.

effects does not exist. Third, actions within this domain occur at computational speed, or near the speed of light. The last unique characteristic is the ability of an attacker to remain anonymous or even to masquerade as another entity. Proxy servers and The Onion Router (TOR) make attribution of an attack difficult, if not impossible (Kallberg and Cook 2017). Further compounding the attribution problem, cyber operations are characterized by a lack of detection by the targets for intelligence gathering and destructive effects until it is too late to defend themselves.

Commanders are guided by doctrine drawn from personal education, experience, or historical context to create an analogy for the current environment (Department of Defense 2011a; Department of the Army 2012). Traditionally, operational commanders come from a combat arms backgrounds at higher levels. Examples of these backgrounds include Infantry, Armor, fighter pilots, naval surface and subsurface fleet commanders. These commanders traditionally lack a computer science or telecommunications education or experience in Signals Intelligence (SIGINT) gathering and analysis. Additionally, commanders are reliant on subjective risk measures that are foundationally based on the experience and education of the commander to assess the operational risks.

Therefore, it is reasonable that commanders and their respective staffs are unable to adequately assess the risks involved, particularly with second and third order effects, for OCO. For example, if an OCO capability is used against a target, several considerations must be considered. First, the capability cannot be used elsewhere globally as an anti-virus company will likely see it and create a signature for it. Next, the target will investigate and remediate the vulnerability used in the OCO. Compounding this consideration is the potential for the vulnerability to vanish globally through remediation. Third, the OCO capability could

potentially be used by the adversary against US targets. Unlike bombs and missiles, OCO capabilities can be reassembled from a forensic investigation and reused. This paper asserts that a new risk assessment technique is needed, one based on quantitative measures that account for the commander's desired operational end-state.

For this research, offensive operations consist of both OCO and intelligence gathering operations. The latter has been at various times identified as computer network exploitation (CNE); intelligence, surveillance, and reconnaissance (ISR), and; surveillance and reconnaissance (S&R). The reason for this deviation from current doctrine is that, from the adversary perspective, attack and intelligence operations look similar, if not the same, until the point of an attack payload is released for effect. This deviation from doctrine also forces consideration on the potential ramifications of detection, attribution, and compromise from adversary actions regardless of the operation.

Current cyber operations

In 2010, U.S. Cyber Command (USCYBERCOM) was established at Ft. Meade, MD, and collocated with the National Security Agency (NSA). Personnel within USCYBERCOM are mostly military with government civilians, and some contractors. Military personnel make up the preponderance of the planning teams for the organization and typically are assigned to USCYBERCOM for three years before returning to their military service career field. It is not unusual for military personnel to be unable to articulate the mechanics of how the Internet works before arriving at USCYBERCOM. However, these same military personnel are on planning teams that support national level interests and support the geographic military combatant commands (CCMD). Currently, CCMDs are responsible for all military operations and therefore, the security of portions of the planet. In February 2014, then Chief of Staff of the Army, GEN Ray Odierno stated that: "We have to be able to do that and potentially be able to conduct tactical offensive cyber operations, because I think in the future, that'll be another way for us to maneuver in the battlespace that we might be in. So I think we have to develop those techniques" (Council on Foreign Relations 2014). However, if the personnel at USCYBERCOM do not understand the risks involved with OCO, how can the CCMDs be expected to make a meaningful assessment of the risks?

Risk assessment methods

Current risk assessment and decision-making for OCO consists of a combination of subjective measurements and other cognitive mechanisms are used in daily routine or simple tasks. However, as complexity rises, or experience diminishes, these cognitive mechanisms begin to fail and initiate other problems. Examples of these mechanisms are group dynamics, heuristics, bias, affect, and overestimation or underestimation of risk.

The systems for risk analysis such as ones used in the Department of Defense (DoD) require extensive experience and knowledge of the risks and consequences involved. The DoD

explains this requirement in the Joint Operations manual that: "Commanders compare similarities of the existing situation with their own experiences or history to distinguish unique features and then tailor innovative and adaptive solutions to each situation." (2017b, II-4, c). Because commanders and their staffs lack experience, education, and expertise in cyberspace operations, these decision-makers are incapable of assessing the risks involved in OCO. Cyber operations have the potential to be considered mixed gambles (Holt and Laury 2002; de Langhe and Puntoni 2015; Kahneman 2013; Kahneman and Lovallo 1993), where both gains and losses may occur simultaneously. This is in contrast with single-domain gambles where only gains or losses may occur (de Langhe and Puntoni 2015).

No existing doctrine for commanding and controlling military operations, much less cyber operations, include the application of multi-criteria decision making for weighing and assessing risks and rewards. Thus, commanders and their staffs are incapable of trading off between reward in operations and the associated costs. This is more vital in cyberspace operations as a superbly executed operation may still not yield the desired end-state of the commander as they will lack perfect knowledge of a target configuration or hardware. The DoD uses fourteen different systems to analyze and assess operational risk (Army War College, personal communication, February 2016). Of these, only four potential systems for assessing risk in cyberwarfare exist: one each from the Army, Navy, Air Force, and Joint doctrine.

The remaining four risk assessment methodologies use subjective terms to convey risk. These systems use terms such as "high," "moderate," or "low" to convey an understanding of the risks and to describe the severity of the risk (Department of the Army 2013; Broder and Tucker 2012). These terms have no clearly defined meaning or context. Often, the definitions of these terms include qualitative descriptions such as "unlikely to occur," "severe impact," and "highly likely" that offer no discrete boundaries to divide and define the areas. Different people may observe the same data and arrive at different conclusions. Consistent metrics do not exist for these measures, which makes this situation even more inexplicable. These risk analysis methodologies are qualitative and ambiguous at best.

Qualitative scales lack standardization and meaning. Two people with different experience levels and backgrounds would likey have different interpretations of what is "severe" or "high impact" (Bennett 2000). This is because non-numeric descriptions lead to different interpretations of data. Budescu, Broomell, and Por (2009) found participants even applied their subjective meaning to the nominal scales, even though a quantified definition existed. However, these subjective meanings were based on the heuristics of each person. Another example of these heuristics at play is the decision maker mentally assigning values, numbers, or probabilities when none exist (Ellsberg 1961). These heuristics consider the bias, past experiences, and cognitive understanding of each person. Therefore, it is impossible for a group of disparate people from different backgrounds and experiences to arrive at the same definition of what constitutes for each level of risk.

Two other flaws of these qualitative systems are range compression and the presumption of regular intervals. In range compression, if numbers are assigned to risk assessments using as an example, a 1–5 or a 1–10 scale, a small incremental movement can have a large impact on the alternatives or consequences. As the scale range decreases, the magnitude of impact conversely increases, that is, if the numbers and the corresponding meanings have regular intervals. With the presumption of regular intervals between levels, a 1–2-3-4-5 scale implies that a 4 is twice as good/bad as a 2; this is not necessarily true (Hubbard 2009; Savage 2012). Alternate methods of overcoming these challenges present their own dilemmas. For example, the Analytical Hierarchy Process (AHP) is often used in multi-criteria decision making. However, AHP suffers from multiple criticisms for use in this manner such as producing arbitrary results (Dyer, 1990) along with a lack of standardized scales for decision maker preferences and an assumption of criteria independence (e.g., no correlation) (Ishizaka, 2009). These flaws make this method substandard for multiple reasons but most importantly, since three of the objectives in the cyber operations hierarchy are dependent on a fourth criterion. The objective hierarchy used in this paper will be discussed in a later section. Since different backgrounds and experiences create different heuristics used to assess the severity of a situation, the current risk assessment systems are inadequate. These inadequate risk assessment systems coupled with the cognitive pitfalls create potential failure when used in new operations where the decision maker and support staff lack the experience and education in understanding the risks and consequences involved.

Cognitive mechanisms

Group dynamics are the interactions of a group setting where one person oversees a decision, but others inform the decision. Two potential problems occur in this situation. First, a strong personality will overrun people that disagree with an opinion. This is a form of confirmation bias. Another potential group dynamic problem is that subordinates will sometimes withhold critical information and defer to the leader even in an emergency. This phenomenon has been identified in multiple workplace environments, to include investigations using flight data recorders of crashed airplanes (Asch 1956, 1955; Gilovich 1991; Garvin and Roberto 2001; de Dreu, Nijstad, and van Knippenberg 2008; Foushee 1982).

Heuristics are the mental rules of thumb and analogies used in everyday life to make sense of new information or to fill in the gaps when information is missing. However, heuristics requires comparable base knowledge for comparison (Kahneman 2003; Dowd, Petrocelli, and Wood 2014; Kane and Webster 2013; Davis, Kulick, and Egner 2005; Grifffin et al. 2002). If a commander perceives the risk of offensive cyber operations as the same as the risk involved in kinetic operations by tanks, aircraft, or ships, this is a flawed comparison. Cyber operations have the potential of the adversary being within your sanctuary to witness and counter your operations on commencement. This aspect does not exist typically in kinetic operations.

Bias is the subjective perception lens that the individual interprets information. Each person uses multiple biases daily. Biases are formed from experiences, education, assumptions, prejudices, and correctly or incorrectly, our observations. Biases are important to consider when data is interpreted to become information. However, multiple people viewing the same data can arrive at different interpretations and contrasting versions of the same information (Kahneman and Tversky 1984; Kahneman 2013, 2003, Tversky and Kahneman 1981, 1974; Davis, Kulick, and Egner 2005; Milkman, Chugh, and Bazerman 2009; Heilbronner, Hayden, and Platt 2010; Dowd, Petrocelli, and Wood 2014; Kane and Webster 2013).

Affect refers to emotions or feelings that sway the judgment of the decision-maker. Examples of such emotions or feelings are fear, anger, surprise, or dread and have a personal value of "goodness" or "badness" (Clore, Gerald L & Huntsinger, Jeffery R, 2007). Cognitive psychology research illustrates how angry people make more aggressive and risk-seeking decisions while fearful or unsure decision makers are more risk-averse. This implies that as decision-makers may make choices that otherwise would be different in other circumstances (Arceneau 2012; Girodo 2007; Kahneman and Tversky 1979; Buelow and Suhr 2013; Bruyneel et al. 2009; Figner et al. 2009; Weber and Chapman 2005; Kahneman and Lovallo 1993; Nygren et al. 1996).

Decision-makers may overestimate risk or be overconfident in the circumstances. A popular example of this phenomenon in research are the people who habitually purchase lottery tickets, but not flood insurance while living in a flood-prone area (Davis, Kulick, and Egner 2005; Heilbronner, Hayden, and Platt 2010; Kahneman and Tversky 1984; Ludvig, Madan, and Spetch 2013; Tversky and Kahneman 1974). Kahneman and Lovallo (1993) describe how individuals manifest overconfidence in themselves when assessing the risk associated with multiple choices. In their study, participants assessed that they were correct approximately 99% of the time when the success rate hovered around 80%. Part of this discrepancy stemmed from optimism.

Operational risks in offensive cyber operations

In military operations, as in the public sector, risk minimization is required. To meet this requirement, the problem and solution set must be optimized to maximize the reduction of risk. Risk management is the process of incorporating the assessment and reduction of risk into decision making. Effective risk management requires the identification of the attributes of concern for the commander and gauging success or failure of each alternative. In OCO, two overarching objectives exist: Maximizing Effectiveness and Minimizing Costs. Effectiveness is a function of the following concerns: Maximizing Intelligence Gained, Maximizing Damage Inflicted, Minimizing Detection of Operations, Minimizing Attribution Given That Detection Occurred, and Minimizing Compromise Given That Detection Occurred (Klipstein 2017). Please refer to Figure 1. Each of these objectives can be further broken down into sub-objectives. However, only the first level of the objective was used in this research.

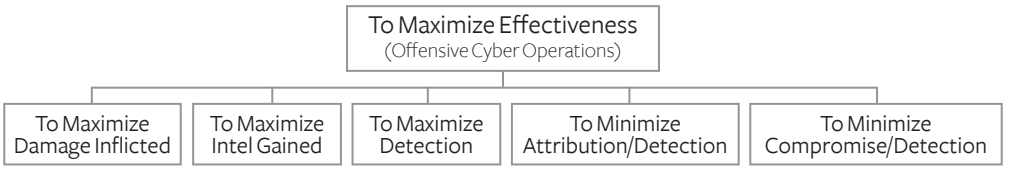


Figure 1. Objective Hierarchy for Maximizing Effectiveness in Offensive Cyber Operations

Maximizing Intelligence Gained and Maximizing Damage Inflicted are self-explanatory for effects the commander wishes to invoke on an adversary. However, operations may be exclusive of each other or in a sequence, depending on the intent of the operation. Minimizing Detection of Operations for this research is defined as the adversary not becoming aware that an intruder has entered their networks. These three elements are value independent of each other.

The next two elements, however, are value dependent on Minimizing Detection of Operations. Minimizing Attribution Given Detection is defined as the adversary being able to reasonably blame a nation or organization for intruding into the adversary network. Minimizing Compromise Given Detection is defined as other friendly operations, by one or more organizations, being discovered and mitigated by the adversary because of initial detection and subsequent investigation. Of note, to maximize the effectiveness of the operation, a minimization may occur as seen in the last three elements.

Similarly, Minimizing Costs can be broken down into Minimizing Personnel Costs, Minimizing Equipment Costs, Minimizing Infrastructure Costs, and Minimizing Time Costs. Personnel Costs are defined as the wages and other costs needed for a workforce. Equipment costs are defined as the distributed resources available for more than one individual. Equipment Costs entail the associated costs of the hardware and software required for creating the software capabilities and modeling the adversary network. Infrastructure Costs include technical actions taken to conduct and protect the cyber operations infrastructure from attribution, including the eventual replacement of infrastructure for redundancy or because of attribution. Time Costs are the last element of the hierarchy. Although time may be monetized to arrive at an incurred cost, such as labor rates, this approach uses a non-monetized definition. In this research, Time Costs are viewed as the length, in days, for a capability to be prepared before an operation commences. Because the first three elements of this hierarchy are classified for cyberwarfare operations by the DoD, only non-monetized time was used as a cost consideration for minimization as shown in Figure 2.

Figure 2. Objective Hierarchy for Minimizing Costs in Offensive Cyber Operations

Current risk assessment techniques are inadequate for commanders to understand the risks involved in cyber warfare. What is needed is a system in which subjective qualitative measures are discarded for quantification. Achieving quantification is best served by multi-criteria decision-making (MCDM) when multiple considerations are used and must be balanced against the decision-maker's values and priorities. For OCO, the risk may be best defined as the failure to meet minimally acceptable measures of effectiveness or to exceed a maximally acceptable level of cost.

Framework

This framework harnesses the experiences of subject-matter experts (SMEs). To qualify as a SME, participants had to possess a minimum of five years with national-level cyber operations. Participant experience in this effort ranged from five to eighteen years with an average of 8.8 years of national-level operations. SME opinions were modeled for each of three courses of action (COA) offered in each scenario with a truncated triangular distribution. This distribution captured what the SME expected to see 90% of the time in the real world. SMEs provided the most likely rate of success to occur, the highest success rate realistically to be expected, and the lowest success rate to be realistically expected. Each SME provided these assessments for any hierarchical element involved. Examples of this are, "What is the likelihood of COA 1 achieving all the required damage?" or "What is the likelihood of COA 1 being detected?"

SME elicitations ranged from 0, never happening, to 1, will always occur, graduated into one-tenth increments. SME uncertainty manifested in the range of the estimation scores provided. For example, if the SME provided the scores: .4, .55, and .6 for lowest value, most likely, and high value respectively, this person has less uncertainty than a SME that provided the scores of .2, .6, and .9 for the same scenario. Therefore, the wider the range or window of scores, the more uncertainty is involved in the elicitation.

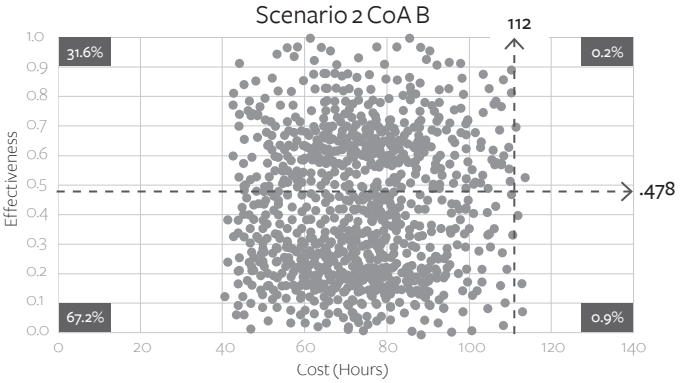


Figure 3. Sample Graphical COA

Since SMEs potentially exhibit the negative cognitive characteristics previously discussed, all SME opinions were equally weighted and then used in a Monte Carlo simulation. The simulation randomly draws SME inputs for each hierarchical concern of the commander. Additionally, the Commander relatively weights concerns to one another. This simulation used the constraints for minimum Effectiveness and the maximum Cost for this operation. Simulations were limited to 3,000 iterations for this research so that later participants could see individual iteration points and how these individual iterations measured against Effectiveness and Cost requirements. Simulations constructed with over 100,000 iterations provided similar distributions; however, the individual iterations of these outputs were indistinguishable. Please see a 3,000 iteration COA simulation output used in Figure 3.

Graphical simulation outputs shown in the Sample COA Evaluation are divided into four regions starting with Region 1 in the upper left corner and then progressing in a clockwise manner. Region 1 is the desired region. In this area, the evaluated course of action meets or exceeds the minimum effectiveness and does not exceed the maximum cost. At the top right is Region 2, where the COA meets the minimum effectiveness but has broken the cost constraint. Below Region 2 is Region 3. In this area, the minimum effectiveness has not been met and the maximum cost has been breached. This is the worst area for a course of action. In the bottom left is Region 4, where the minimum effectiveness has not been met, but the maximum cost has not been exceeded.

Experiment

This research effort elicited the participation of offensive cyber planners at each CCMD, resulting in 60 of the 61 available planners participating. Participants were given a scenario set in five years in the future. In these scenarios, authority to conduct OCO had been delegated to the CCMD with USCYBERCOM conducting deconfliction. Adversaries ranged from peer-state, less advanced nations, and non-nation state actors. Participants were presented with three attacking and three intelligence gathering scenarios. In each scenario, participants had to rank the order of the three COA's based on the commander's guidance for operational goals, desired end-state, and concerns.

Planners read each scenario and the written descriptions of each COA before rank ordering the COA. Participants were then presented with a second group of COA in a graphical format. Participants were told that the graphical COA had no bearing on the written COA. In truth, the graphical COA was the mathematical representation of the written COA based on SME elicitations. Graphical COA were placed in a randomized order to further obfuscate the relation between the two groups. Participants then rank ordered the graphical COA based on the same commander's guidance from the written COA.

Commander preferences for operational goals and tolerances of risk were mathematically modeled using mid-value splitting techniques (Kirkwood 1997). This allows for tradeoff values between operational goals, as defined by the hierarchical objectives previously dis-

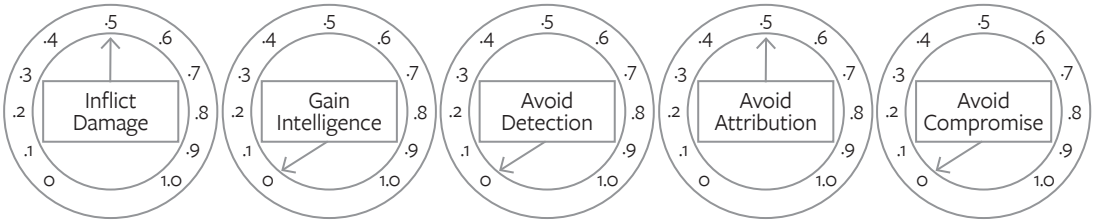


Figure 4. Example Dials for Adjusting for Decision Maker Weight for a Given Operation (Klipstein, 2017)

cussed. The result is a language that allows the commander to fine-tune objectives concerning each other. In the example illustrated in Figure 2, the commander places equal weight on inflicting damage and avoiding attribution. All other hierarchical goals are accounted for with a weight of zero. Commanders may weigh any objective as they wish so long as the total of the five objectives does not exceed 1, the total amount of "care" of the commander.

RESULTS

This research effort investigated how useful a framework with graphical outputs of risk is for aiding personnel who lack the necessary experience. In this effort, the personnel examined were two groups: personnel with national level cyber experience and personnel without national cyber level experience. The experiment focused on the amount of change between the rankings of written and graphical COAs.

This effort determined that 22 of the 36 analyses undertaken met or exceeded statistical significance, suggesting that a framework built on SME knowledge and expertise that incorporated the uncertainty that SMEs acknowledge allowed decision makers to make more informed assessments of risk, and consequently, better decisions regarding unfamiliar and new operations within their organizations. This research succeeded in creating a tailor-made expression of risk based on the Commander's preferences and desires.

Each scenario was analyzed in six different ways. The first three ways are as follows: all participants with no one group, either national level experienced or inexperienced, held constant; all participants with personnel with national level experience held constant; and all participants with personnel lacking national level experience held constant. These three analyses are used for two reasons. The first is to determine if the framework benefits the population. The second is to determine if the increased participant size affects the outcome of the experiment.

The fourth scenario consisted solely of participants with previous national-level experience. The fifth is the converse: personnel lacking national level experience. The sixth analysis focused on USCYBERCOM participants. This analysis examines how effective this framework is for planners currently working at the national level, in addition to being used as the control for comparison against inexperienced personnel. For this paper, only a comparison of

experienced personnel as a group, inexperienced personnel as a group, and USCYBERCOM planners occurs.

Scenario 1A

Scenario 1A introduced the participants to a future scenario in which CCMDs have been partially delegated authority to conduct intelligence and conduct offensive cyber operations. In this first scenario, the combatant commander needs intelligence to ascertain the intentions of an adversary that is threatening a US ally and escalating tensions. Intelligence from other sources indicates the adversary may invade the ally, and the combatant commander wishes to confirm the reports. In this scenario, the commander places values of 60% for avoiding detection, and 40% for gathering the required intelligence. Success in this operation is defined as the exfiltration of a Microsoft Word document outlining the adversary's attack plans, at a minimum.

In retrospect, the COAs for this scenario may have been too similar in their predicted probability of success. Multiple participants noted the potential for detection in the written COAs. COA B, the most popular first choice, was not detected in virtualized testing. The next most popular written COA choice was COA C, which had been used in operations in the past undetected, but virtualized testing indicated that it would be detected. The least popular choice, COA A, was a modified open-source tool with a known signature that offered a 50/50 chance of detection. This information also aligns with the Graphic COA choices.

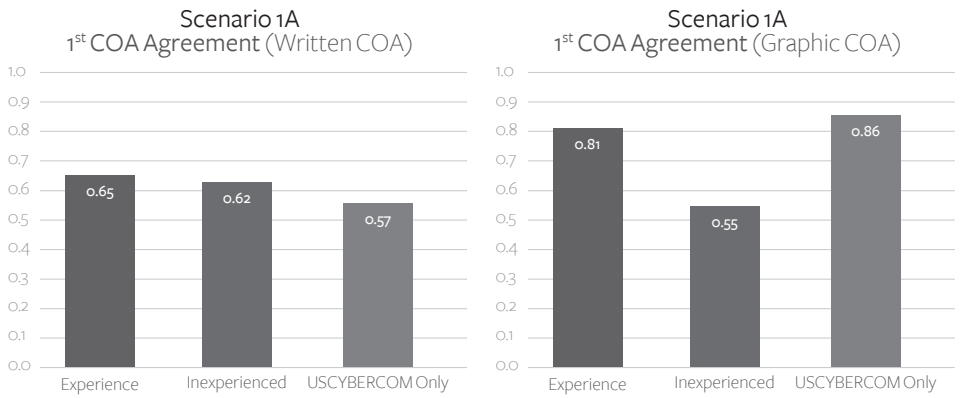


Figure 5. Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 1A

Analysis of the graphical choices made by participants demonstrates that COA B, presented to the participants as COA 3, was the overwhelming first choice in every analysis. COA B had a combined 27.7% predicted effectiveness when Regions 1 and 2 were combined. The second choice in all but two analyses was COA A, also presented as COA A. Not enough data exists in this scenario to accurately account for choices made between the other two COAs when examining second and third choices. As statistical significance was not attained in any

of the analyses in this scenario, no further analysis will be conducted to illustrate support for the advanced hypothesis. Please refer to Figure 5 for the rate of first choice COA agreement for both written and graphic COAs. Although not statistically significant, both the experienced personnel and the USCYBERCOM only groups increased in the aggregated consensus of what the first COA for a recommendation for implementation should be.

Scenario 1B

Scenario 1B is the escalation of Scenario 1A. In this scenario, the commander has attained the required information. Analysis has determined that the adversary intends to erode the trust between the US and its ally by conducting small-scale guerilla attacks. The commander wishes to conduct OCO for two purposes: to disrupt the planning for guerrilla attacks and to demonstrate the network vulnerabilities to the adversary, suggesting that the US is aware of its intentions. The commander places 60% of his value on destruction and 40% on avoiding attribution. Success in this operation is achieved when all information residing on the target containing a one terabyte hard drive is rendered inaccessible and unrecoverable.

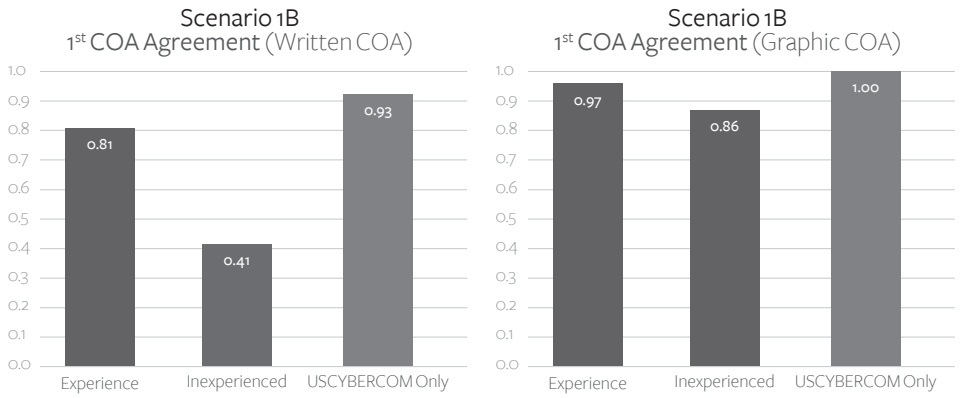


Figure 6 - Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 1B

Figure 6 demonstrates the ability of this framework to aid all personnel with national level experience in understanding risk, not just the inexperienced. In this scenario, the result was not only an increase in aggregated consensus across all three groups but also a change in the primary recommended COA to the commander. Additionally, this scenario demonstrated how a COA might be interpreted as feasible in a written format while having little to no potential for success when mathematically modeled. Remember that thirty SMEs evaluated the different COAs and provided their 90% confidence intervals. This insight further demonstrates the need for quantified risk analysis. Participants, regardless of the method of analysis, continued to make decisions of preference ranking based on Region 1 of the charts, as was observed in Scenario 1A.

Scenario 2

Scenario 2 changes the focus to combating a non-state actor. In this scenario, the actor in

question uses the Internet to recruit, to spread propaganda, and to orchestrate command and control of operations. The non-state actor escalates the situation by posting a video of a captured US military member being killed as a propaganda tool. The combatant commander, working in coordination with the Theater Special Operations Command (TSOC), designated five personnel as high payoff targets. The targeted personnel are instrumental to operations and are believed to be directly connected to the service member's death. For this operation, the combatant commander orders that online intelligence operations are to commence to gather information for ascertaining the patterns of life of the five targets. Once enough information has been attained, the TSOC will coordinate for capture/kill operations to commence. The combatant commander has placed equal value on gaining intelligence while avoiding detection.

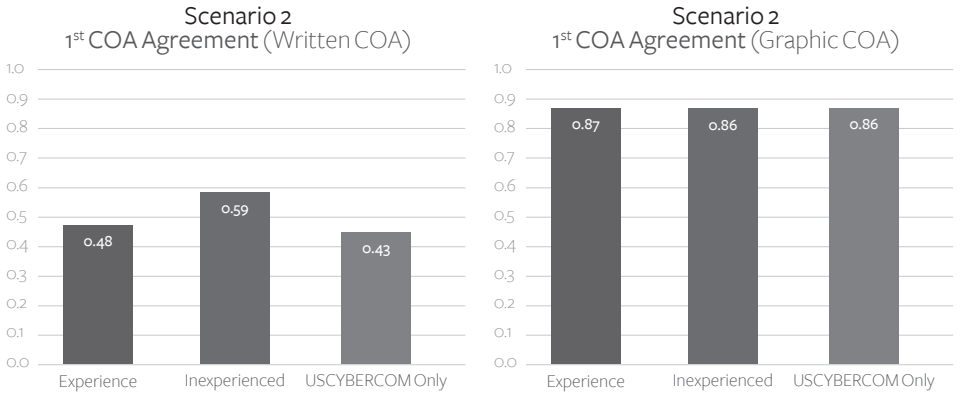


Figure 7. Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 2

As in previous scenarios, the results suggest that participants use Region 1 of the graphics as a tool for assessing preference. This scenario further reinforces the hypothesis that a framework built on SME insights, which quantifies risk, and that presents results in a graphical output can mitigate the inexperience of cyber planners when compared to those with national level experience. In the graphic COAs, 86% of the inexperienced personnel chose the same first preferred COA. This percentage is comparable to the 87% of the overall national level experienced planners and 85% for the USCYBERCOM only planners.

Scenario 3

Scenario 3 presents the participants with another intelligence-gathering operation. In this scenario, an adversarial government uses state-sponsored contracted companies to work on the government's behalf in an attempt to avoid attribution. Intelligence indicates that the contracted company has infiltrated the combatant command networks and exfiltrated documents that update the Theater Security Cooperation agreements, to include personnel and equipment movement schedules and locations.

The commander orders an intelligence operation to confirm or deny the presence of sensitive U.S. military documents within the adversary's network. Confirmation in this operation

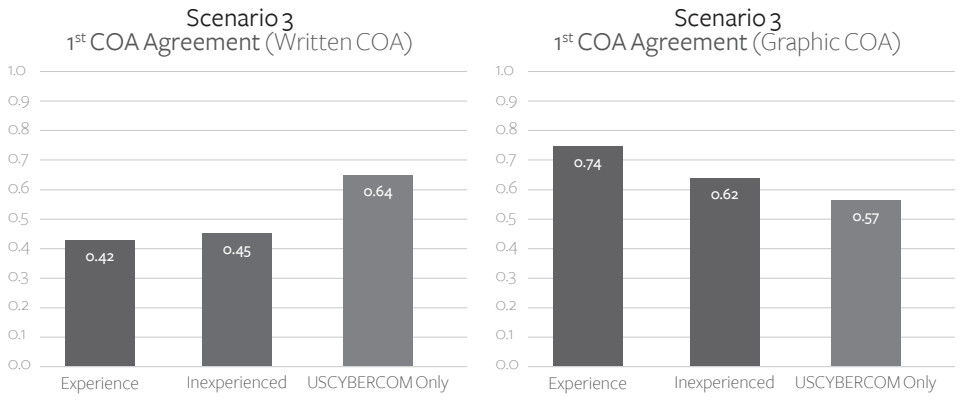


Figure 8. Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 3

is defined as the identification of the 400MB of the non-public portion of the Theater Security Agreement, which ranges in classification from SECRET to TOP SECRET. This operation will be considered a success if all 400MB of the sensitive portion of the document is identified, copied, and downloaded. Notably, OCO action is not authorized at this time.

Analysis of the command's networks indicates that at least two adversary entry points exist and that more are probable. As such, the commander places a value of 60% on avoiding attribution due to the sophistication of the adversary. As the adversary uses state-sponsored contracted companies for operations, the commander also wishes to prevent attribution to the company that works on the adversary's behalf. The remaining 40% of the commander's value comes from the intelligence potentially gained.

As in previous scenarios, indications suggest that participants continue to use Region 1 of the graphics as a tool for assessing preference. All three groups again shifted in the primary COA selection from A to B. In this scenario; the recommended graphic COA had only a 12% predicted success from the simulation compared to 7.1% for the second choice and 2.3% for the third. In the graphic COAs, 62% of the personnel lacking national level experience chose the same first preferred COA. This result is comparable to the 74% of the overall national level experienced planners and 57% for the USCYBERCOM only planners. Due to the groups' 33% increased agreement on COA B being the recommended COA, Scenario 3 again supports the hypothesis advanced by this research.

Scenario 4

In this scenario, the CCMD, in coordination with the CIA, plans to conduct OCO against a non-state actor's online magazine before being published in two weeks. This operation serves two purposes: to prevent disseminating bomb-making information in the magazine and to facilitate the CIA identification of the magazine's readers. Due to other unrelated CIA activities within web forums, the commander has been directed not to bring attribution to US or CIA efforts. Because of this directive, the commander values the outcomes of this operation

at 40% for the destruction or denial of the online material, 30% for avoiding attribution, and 30% for avoiding compromise.

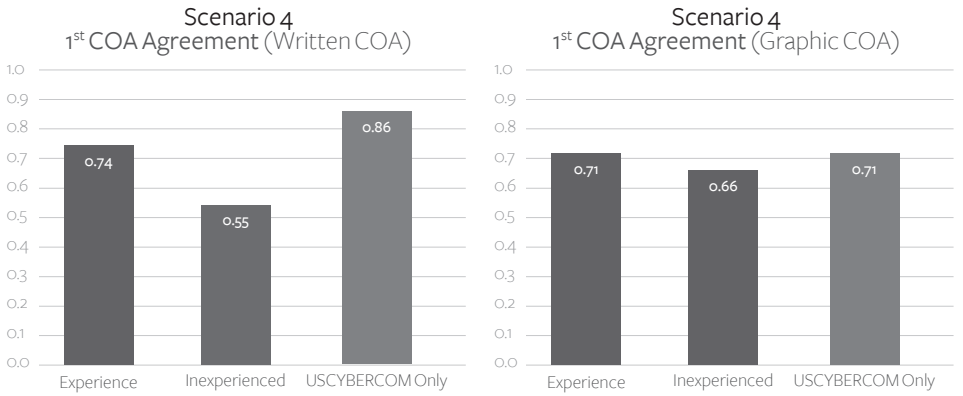


Figure 9. Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 4

Analysis of the outcomes of this scenario suggests two pieces of information were used to rank order COAs. First, the graphic Region 1 prediction matches the written COA ranking. Second, the participant packets showed that participants indicated—using underlining, circling, and highlighting—key information in the written COAs used for decision making. This information pertained to the likelihood of a capability being detected during the operation. The rankings are given in order from least likely to be detected to most likely, matched the written rankings and the graphical Region 1 prediction of success, from most likely to least. Thus, the participants were able to assume the proper ranking of COAs most likely to be based on the written format, suggesting that this scenario suffers from a design flaw. See Figure 9.

Scenario 5

The last scenario for the participants portrays another OCO operation. An adversary of the US uses a state-sponsored business to conduct operations on its behalf. The business in question has targeted US and allied systems with malware for intelligence gathering and denial of service. Additionally, these attacks have been highly publicized in the media but not publicly attributed due to US intelligence equities.

The planned OCO operation will demonstrate to both the adversary and the state-sponsored business that the US is knowledgeable of the adversary's activities. However, US cyber operations must prevent the adversary from discovering and attributing the network infrastructure used for these operations. For these reasons, the commander places 50% of the value of the operation on attaining destruction, 30% on avoiding detection, and 20% on avoiding attribution.

This scenario suggests that participants use Region 1 and Region 2 of the graphics as a tool for assessing preference as observed in Scenario 1A. Again, participants in the aggregate

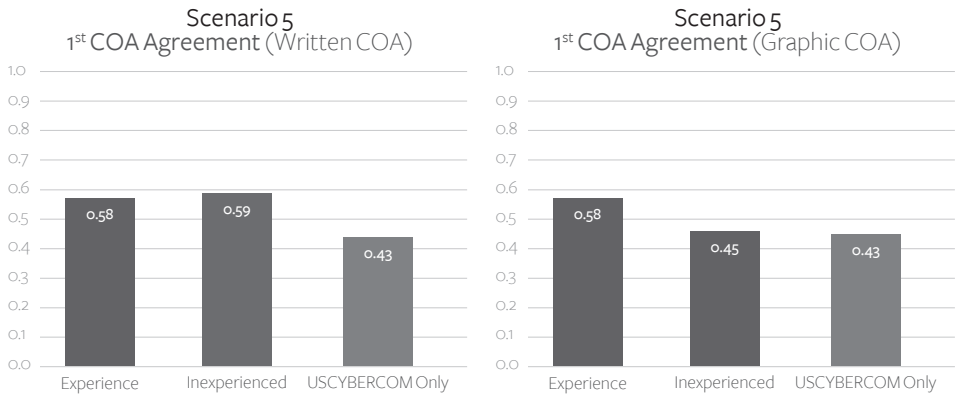


Figure 10. Percentage of 1st Choice COA for Written and Graphic COAs in Scenario 4

changed what COA would be recommended for implementation, from COA B to COA A. This method in which decision makers prioritize data for decision merits further research. In the graphic COAs, 44% of the inexperienced personnel chose the same first preferred COA. This is lower than the 58% of the overall national level experienced planners. Since the USCYBERCOM-only planner analysis was not statistically significant and will not be compared, this result further suggests that the hypothesis is supported. Please refer to Figure 10.

ANALYSIS

The analysis of the collected data uncovered three trends. First, inexperienced personnel overcame their lack of national-level experience and made decisions on par with experienced personnel. Next, using the framework, experienced personnel more often expressed preferences for the same decision and subsequent action. Third, the data suggest that Region 1 in the graphics was the primary determining factor for the decision.

Inexperienced personnel overcome their lack of experience

The first trend identified was the goal of the research, namely, to overcome the lack of national-level experience at organizations below the national-level for OCO. Inexperienced personnel lack a thorough understanding of the environment, along with second and third order effects of operations. For this analysis, inexperienced offensive cyber planners made decisions on par with experienced offensive cyber planners, in addition to offensive planners currently working at USCYBERCOM.

Inexperienced personnel were more likely to agree on a recommended COA in graphical form versus written form in four of six scenarios. The increase in agreement ranged from 18% in Scenario 4 to 47% in Scenario 2. Inexperienced personnel recorded a negative change in agreement, -11%, for the preferred COA while the experienced group and the USCYBERCOM planners both recorded a 50% increase and 25% increase, respectively. Interestingly, the inexperienced personnel bested the experienced and USCYBERCOM personnel in Scenario 1B.

In this scenario, the inexperienced personnel recorded a 33% increase in agreement on the preferred COA while the experienced personnel decreased by 28% and the USCYBERCOM planners decreased by a remarkable 46%.

Scenario 5 was the other scenario in which the inexperienced personnel did not increase in agreement on the preferred COA. In Scenario 5, the inexperienced personnel decreased in agreement by 23%, and as a group changed their preferred COA selection from the written to the graphic. Conversely, the experienced personnel registered no change in the level of agreement, but a change in COA selection. The USCYBERCOM planners as a subset also had no change in their level of agreement but a change in COA selection.

Additionally, the data suggests that the graphics produced by this quantitative framework mitigate the lack of national-level experience possessed by the inexperienced personnel. In the four scenarios that exceeded a 95% confidence interval, inexperienced personnel selected the same COA in comparable numbers to the experienced personnel and the USCYBERCOM planners. For Scenario 1B, the inexperienced personnel chose COA B at a rate of 55%, on par with 58% of the experienced personnel and 50% of the USCYBERCOM planners. Scenario 2 resulted in 86% of the inexperienced personnel choosing COA A along with 87% of the experienced personnel and 85% of the USCYBERCOM planners. Scenario 3 resulted in the USCYBERCOM planners not meeting or exceeding a 95% confidence interval; however, 62% of the inexperienced personnel selected COA B while 74% of the experienced group also did. In Scenario 5, the USCYBERCOM planners again did not exceed a 95% confidence interval. However, 44% of the inexperienced personnel opted for COA C as the primary choice while 58% of the experienced group chose COA A. This analysis suggests that although the hypothesis is supported regarding mitigating the lack of national-level expertise, the framework may also aid experienced personnel.

Value for experienced personnel

Experienced personnel exhibited greater agreement in selecting the first recommended COA when comparing the amount of consensus from the written to the graphic COA. They increased in agreement in four scenarios. Most remarkably, in Scenario 2, they increased in agreement by 80% and in Scenario 3 by 53%. Additionally, the USCYBERCOM planners increased their agreement in three scenarios. Most notably, the agreement for COA recommendation in Scenario 2 doubled. In Scenario 1A, the agreement increased by 50%. Additionally, a quantified framework may be of use in USCYBERCOM if offensive planners continue to rotate out of the organization at the current rate of two to three years.

USCYBERCOM is a military organization working at the national-level of cyber operations, employing both military and civilian personnel. As such, the average military planner leaves this assignment in three years, sometimes two. It is also not unusual for planners to come from diverse backgrounds into USCYBERCOM with no prior experience in cyber operations. Given this, the mean USCYBERCOM experience at the national-level is 3.78 years, less than

the five years needed for an expert status by this research effort and by many other mainstream researchers (Ericsson, Prietula, and Cokely 2007; Prietula and Simon 1989; Macnamara, Hambrick, and Oswald 2014; Ericsson, Krampe, and Tesch-Romer 1993). Only five of the 14 USCYBERCOM planners have a minimum of five years' experience to meet this standard. Three of the five personnel who meet this five-year, expert-level standard are civilians. This unexpected result suggests that the framework is useful for the less experienced national level personnel as well.

Use of Region 1 for decision making

As mentioned in the previous chapter, the data suggests that participants, both with and without national-level experience, typically relied on Region 1 of the graphic representation for a rank preference decision. Recall that Region 1 is the quadrant of the graph that satisfies both the effectiveness and cost requirements of the commander. This suggestion was further reinforced by an examination of the COA ranking choices participants made. The selections of inexperienced personnel, experienced personnel, and USCYBERCOM personnel aligned with the highest Region 1 value in the CoAs for Scenarios 1B, 2, and 4. Additionally, the second and third COA ranking aligned to the second and third highest percentages of predicted success in Region 1 of the CoAs. Furthermore, the USCYBERCOM planners' choices aligned to the highest Region 1 value in Scenario 5.

In two of the scenarios, participants combined the predicted success scores of Regions 1 and 2 to rank their preferences. Region 2 meets the minimum effectiveness of the commander but goes past the maximum time allowed. In Scenarios 1A and 5, except for the USCYBERCOM planners in Scenario 5, participant rankings aligned with the combined scores of Regions 1 and 2. The first preferred COA aligned with the highest combined score, the second with the next highest, and so on. This suggested technique would focus on the effectiveness of a capability without regard to the cost in time. Therefore, the participant only thinks about the end state, not the cost. These findings must be subject to formal testing, however, if they are to be taken as indicative of general decision behavior.

CONCLUSION

This research effort set out to test the hypothesis that a quantifiable framework could mitigate the lack of national-level expertise for OCO at the CCMDs. The outcome is a highly effective framework that considers the operational desires, risk tolerances, and personal values for individual decision makers. This framework uses insights of SME expertise to give a more complete and unbiased view of the probability of success regarding mission effectiveness and the predicted costs. Not only did this research support the hypothesis, but it also has its own unexpected utility for experienced personnel in organizations below the national level and the current USCYBERCOM planners. This framework demonstrated that inexperienced organizations have the potential for making decisions on par with experienced organizations, given that a quantifiable framework and SME insights are available.

NOTES

Arceneau, Kevin, 2012, Cognitive Biases and the Strength of Political Arguments, *American Journal of Political Science,* 56 (2), 271–85.

Asch, Solomon E., 1955, Opinions and Social Pressure, *Scientific American* 193 (5), 2–6.

——. 1956 Studies of Independence and Conformity: I. A Minority of One against a Unanimous Majority, *Psychological Monographs: General and Applied* 70 (9), 1–70. https://doi.org/http://dx.doi.org.libproxy.nps.edu/10.1037/h0093718.

Bennett, Ruth, 2000, Risky Business The Science of Decision Making Grapples with Sex, Race, and Power, *Science News* 158 (12), 190–91, http://www.jstor.org/stable/3981298.

Broder, James F, and Eugene Tucker, 2012, *Risk Analysis and the Security Survey,* 4th ed. Oxford: Butterworth-Heinemann.

Bruyneel, Sabrina D, Siegfried Dewitte, Philip H Franses, and Marnik G Dekimpe, 2009, I Felt Low and My Purse Feels Light : Depleting Mood Regulation Attempts Affect Risk Decision Making, *Journal of Behavioral Decision Making* 170 (October 2008), 153–70, https://doi.org/10.1002/bdm.

Budescu, David V. (University of Illinois at Urbana-Champaign), Stephen Broomell (University of Illinois at Urbana-Champaign), and Han-Hui Por (University of Illinois at Urbana-Champaign), 2009, Improving Communication of Uncertainty in the Reports of the Intergovernmental Panel on Climate Change, *Psychological Science* 20 (3), 299–308.

Buelow, Melissa T., and Julie A. Suhr, 2013, Personality Characteristics and State Mood Influence Individual Deck Selections on the Iowa Gambling Task, *Personality and Individual Differences* 54 (5), 593–97, https://doi.org/10.1016/j.paid.2012.11.019.

Clore, Gerald L (University of Virginia), and Huntsinger, Jeffery R. (University of Virginia), 2007, How Emotions Inform Judgment and Regulate Thought, *Trends in Cognitive Sciences* 11 (9), 393–99, https://doi.org/10.1016(J.tics.2007.08.005.

Council on Foreign Relations, 2014, Amid Tighter Budgets, U.S. Army Rebalancing and Refocusing - Council on Foreign Relations." *Transcripts.* http://www.cfr.org/united-states/amid-tighter-budgets-us-army-rebalancing-refocusing/p32373.

Davis, Paul K, Jonathan Kulick, and Michael Egner, 2005, Implications of Modern Decision Science for Military Decision-Support Systems, Arlington, VA: RAND.

de Dreu, Carsten K W, Bernard A Nijstad, and Daan van Knippenberg, 2008, Motivated Information Processing in Group Judgment and Decision Making, *Personality and Social Psychology Review: An Official Journal of the Society for Personality and Social Psychology, Inc 12* (1), 22–49, https://doi.org/10.1177/1088868307304092.

de Langhe, Bart, and Stefano Puntoni, 2015, Bang for the Buck: Gain-Loss Ratio as a Driver of Judgement and Choice, *Management Science* 61 (5), 1137–63.

Department of Defense, 2017a, *Joint Operations,* Washington D.C.

——, 2017b, Joint Operations, Washington D.C.: Department of Defense.

Department of the Army, 2012, ADP 6-0 (*Mission Command*), Washington D.C.: Army Publishing Directorate, https://armypubs.us.army.mil/doctrine/index.html.

——, 2013, AR 385-10 *The Army Safety Program*, Washington D.C.: Army Publishing Directorate.

Dowd, Keith W, John V Petrocelli, and Myles T Wood, 2014, Integrating Information from Multiple Sources: A Metacognitive Account of Self-Generated and Externally Provided Anchors, *Thinking & Reasoning* 20 (3). Department of Psychology, Wake Forest University, Winston-Salem, NC, US petrocjv@wfu.edu; Petrocelli, John V.,P.O. Box 7778,Winston-Salem,US,27109,Department of Psychology, Wake Forest University,petrocjv@wfu.edu: Taylor & Francis, 315–32, https://doi.org/http://dx.doi.org/10.1080/13546783.2013.811442.

Ellsberg, D., 1961, Risk, Ambiguity, and the Savage Axioms, *Quarterly Journal of Economics* 75 (November), Unlisted:643–69, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/864366624?accountid=12702.

Ericsson, K. Anders, Ralf Krampe, and Clemens Tesch-Romer, 1993, The Role of Deliberate Practice in the Acquisition of Expert Performance, *Psychological Review* 100 (3), 363–404, https://doi.org/0033-295X/93.

Ericsson, K Anders, Michael Prietula, and Edward Cokely, 2007, The Making of an Expert, *Harvard Business Review* July-Augus, 1–7.

Figner, Bernd, Rachael J. Mackinlay, Friedrich Wilkening, and Elke U. Weber, 2009, Affective and Deliberative Processes in Risky Choice: Age Differences In Risk Taking in the Columbia Card Task, *Journal of Experimental Psychology: Learning, Memory, and Cognition* 35 (3), 709–30, https://doi.org/http://dx.doi.org/10.1037/a0014983.

Foushee, H C. 1982, The Role of Communications, Socio-Psychological, and Personality Factors in the Maintenance of Crew Coordination, *Aviation, Space, and Environmental Medicine* 53 (11), 1062–66, http://www.researchgate.net/publication/16049243_The_role_of_communications_socio-psychological_and_personality_factors_in_the_maintenance_of_crew_coordination.

NOTES

Garvin, David A, and Michael A Roberto, 2001, What You Don't Know About Making Decisions, *Harvard Business Review* September, 22–32.

Gilovich, Thomas, 1991, *How We Know What Isn't So.* New York, NY: The Free Press.

Girodo, Michel, 2007, Personality and Cognitive Processes in Life and Death Decision Making: An Exploration into the Source of Judgment Errors by Police Special Squads, *International Journal of Psychology* 42 (6), University of Ottawa, Ottawa, ON, Canada girodo@uottawa.ca; Girodo, Michel,145 Jean-Jacques Lussier Street,Ottawa,Canada,K1N 6N5,School of Psychology, University of Ottawa,girodo@uottawa.ca: Taylor & Francis Wiley-Blackwell Publishing Ltd., 418–26, https://doi.org/http://dx.doi.org/10.1080/00207590701436728.

Grifffin, Robert J, Kurt Neuwirth, James Giese, and Sharon Dunwoody. 2002, Linking the Heuristic-Systematic Model and Depth of Processing, Communication Research. 2002, https://doi.org/10.1177/009365002237833.

Heilbronner, Sarah R., Benjamin Y. Hayden, and Michael L. Platt, 2010, Neuroeconomics of Risk-Sensitive Decision Making, In *Impulsivity: The Behavioral and Neurological Science of Discounting,* edited by Gregory Madden, PhD and Warren Bickel, PhD, 159–87, American Psychological Association.

Holt, Charles A, and Susan K Laury, 2002, Risk Aversion and Incentive Effects, *The American Economic Review* 92 (5). Nashville: American Economic Association, 1644–55. http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/233033790?accountid=12702.

Hubbard, Douglas W. 2009, Worse Than Useless: The Most Popular Risk Assessment Method and Why It Doesn't Work, In *The Failure of Risk Management: Why It's Broken and How to Fix It,* 117–43, Hoboken, NJ: John Wiley & Sons.

Kahneman, Daniel, 2003, A Perspective on Judgement and Choice, *American Psychologist* 58 (9), 697–720, https://doi.org/10.1037/0003-066X.58.9.697.

——. 2013, Thinking Fast and Slow, 2nded, Farrar, Straus and Giroux.

Kahneman, Daniel, and Dan Lovallo, 1993, Timid Choices and Bold Forecasts - a Cognitive Perspective on Risk Taking, *Management Science* 39 (1), 17–31, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/38481183?accountid=12702.

Kahneman, Daniel, and Amos Tversky, 1979, Prospect Theory: An Analysis of Decision under Risk." *Econometrica* 47 (2), 263–91, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/56137572?accountid=12702.

——, 1984, Choices, Values, and Frames, *American Psychologist* 39 (4):341–50.

Kallberg, Jan, and Thomas Cook, 2017, The Unfitness of Tradional Military Thinking in Cyber, IEEE Access 5, 8126–30.

Kane, Joanne, and Gregory D. Webster, 2013, Heuristics and Biases That Help and Hinder Scientists: Toward a Psychology of Scientific Judgment and Decision Making, In *Handbook of the Psychology of Science,* edited by Gregory PhD Feist and Michael PhD Gorman, 1sted., 437–59, New York, NY: Springer.

Kirkwood, Craig, 1997, *Strategic Decision Making,* Edited by Carl Hinrichs, Belmont, CA: Wadsworth Publishing Company.

Klipstein, Michael. 2017, Quantifying Risk for Offensive Cyber Operations, Naval Postgraduate School.

Ludvig, Elliot A. (Princeton University), Christopher R. Madan (University of Alberta), and Marcia L. Spetch (Universtiy Medical Center Hamburg-Eppendorf), 2013, Extreme Outcomes Sway Risky Decisions from Experience, *Journal of Behavioral Decision Making* 27, 146–56, https://doi.org/10.1002/bdm.1792.

Macnamara, Brooke, David Hambrick, and Frederick Oswald, 2014, Deliberate Practice and Performance inMusic, Sports, Education, and Professions: A Meta-Analysisle, *Association for Psychological Science*2 25 (8), 1608–18.

Milkman, Katherine L, Dolly Chugh, and Max H Bazerman, 2009, How Can Decision Making Be Improved?, *Perspectives on Psychological Science* 4 (4), University of Pennsylvania, Philadelphia, PA, US kmilkman@wharton.upenn.edu; New York University, New York, NY, US ; Harvard University, Cambridge, MA, US; Milkman, Katherine L.,500 Jon M. Huntsman Hall,Philadelphia,US,19104,Wharton School, University of: Wiley-Blackwell Publishing Ltd. Blackwell Publishing Sage Publications, 379–83, https://doi.org/http://dx.doi.org/10.1111/j.1745-6924.2009.01142.x.

Nygren, Thomas E, Alice M Isen, Pamela J Taylor, and Jessica Dulin, 1996, The Influence of Positive Affect on the Decision Rule in Risk Situations: Focus on Outcome (and Especially Avoidance of Loss) rather than Probability, *Organizational Behavior and Human Decision Processes* 66 (1), New York: Elsevier Science Publishing Company, Inc., 59, http://libproxy.nps.edu/login?url=http://search.proquest.com/docview/223179153?accountid=12702.

Prietula, Michael, and Herbert Simon, 1989, The Experts in Your Midst, *Harvard Business Review,* no. January-February 1989, 120–24.

NOTES

Savage, Sam, 2012, *The Flaw of Averages*, Hoboken, NJ: Wiley.

Tversky, Amos, and Daniel Kahneman, 1974, Judgment under Uncertainty: Heuristics and Biases, *Science* 185 (4157), Hebrew U, Jerusalem, Israel: American Assn for the Advancement of Science, 1124–31, https://doi.org/http://dx.doi.org/10.1126/science.185.4157.1124.

Tversky, Amos, and Daniel Kahneman, 1981, The Framing of Decisions and the Psychology of Choice, *Science* 211 (4481), Stanford U: American Assn for the Advancement of Science, 453–58, https://doi.org/http://dx.doi.org/10.1126/science.7455683.

Weber, Bethany J, and Gretchen B Chapman, 2005, Playing for Peanuts: Why Is Risk Seeking More Common for Low-Stakes Gambles?, *Organizational Behavior and Human Decision Processes* 97 (1), Psychology Department, Rutgers University, Piscataway, NJ, US bweber@eden.rutgers.edu; Weber, Bethany J.,152 Frelinghuysen Road,Piscataway,US,08854-8020,Psychology Department, Rutgers University,bweber@eden.rutgers.edu: Elsevier Science, 31–46, https://doi.org/http://dx.doi.org/10.1016/j.obhdp.2005.03.001.

Cyber Attribution: Can a New Institution Achieve Transnational Credibility?

Milton Mueller
Karl Grindal
Brenden Kuerbis
Farzaneh Badiei

INTRODUCTION

After the United States blamed China for the Office of Personnel Management intrusion in 2015, China called speculation on their involvement neither "responsible nor scientific." [1] They subsequently suggested it was "imperative to stop groundless accusations, [and] step up consultations to formulate an international code of conduct..." [2] The US-China exchange raises a critical question: what qualifies as "groundless accusations," and what would "responsible and scientific" attribution of nation-state sponsored attacks look like? The incident raises another question as well: what is the current US process for attribution, and is it achieving its aims? This paper argues that authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New, credible institutions are needed to develop procedural checks and balances that will make attribution more than one nation pointing its finger at an adversary. This document will explore the attribution challenge, review proposed models for new institutions, and sketch an agenda for future research. The authors' expertise in the development of transnational institutions led by non-state actors in critical Internet resources has direct policy relevance to this case, as a new institution may be needed to hold offensive actors responsible and deter future cyber-attacks.

The role of cyber attribution in deterrence and accountability

One can defend against a cyber-attack, but without attribution, attackers lack a deterrent. At best, secure systems increase the amount of time it takes an attacker to find a vulnerability to a point beyond that which the attacker is willing to spend. Without proper incentives to restrain malicious attacker behavior, be they state or non-state, it is unreasonable to expect the present situation to change.

Milton L Mueller is Professor at the Georgia Institute of Technology (Atlanta, USA) in the School of Public Policy. He is the author of Will the Internet Fragment? (Polity, 2017), Networks and States: The global politics of Internet governance (MIT Press, 2010) and Ruling the Root: Internet Governance and the Taming of Cyberspace (MIT Press, 2002) are acclaimed scholarly accounts of the global governance regime emerging around the Internet.

Accurate attribution requires experienced threat intelligence and digital forensics experts advising decision-makers. While governments and threat intelligence groups will attribute attacks to specific intrusion sets, sometimes even linking these to specific actors, no internationally recognized forensic process with an evidentiary based level of confidence exists. Rather, attribution is often based on limited evidence and the reputation of the attributing entity. How can we expect a global coalition to implement sanctions when attributing groups and attackers could be based anywhere in the world, and there is no recognized standard or institutionalized process for attribution?

There is an important distinction between identifying intrusion sets and assigning them to an adversary or "threat group," and linking this adversary with a known state or non-state actor. Robert Lee refers to the latter as "true attribution." [3] This two-part distinction can be compared to Herb Lin's model, developed in the paper *Attribution of Malicious Cyber Incidents*, [4] which uses three levels of attribution: machines, human operators, and the ultimately responsible party. In Mandiant's 2013 attribution of APT-1 to the Chinese People's Liberation Army (PLA) Unit 612398 [5] all three levels of Lin's model are described. At the lowest level would be the IP addresses associated with command and control servers. Next is attribution to a human operator—the Mandiant report identifies a person who went by the alias "ugly gorilla" and associated this alias with the real person Wang Dong. Ultimately, the report attributed APT-1 to the PLA hence, the Chinese state.

Defining the ultimately responsible party can be particularly challenging when it comes to state involvement. Even when a person has been clearly identified as being inside or a citizen of the attributed country, it may not be clear from the forensics whether that person is a contractor, or an employee operating at the behest

Karl Grindal is a Ph.D. Student at the Georgia Institute of Technology's School of Public Policy and partner with the Internet Governance Project. Karl previously served as a Senior Analyst at Delta Risk LLC and as the Executive Director of the Cyber Conflict Studies Association (CCSA), a non-profit dedicated to advancing a research agenda on cyber conflict.

of their national government or operating on their own. Jason Healey's "Spectrum of State Responsibility" acknowledges that states employ hackers, contract out hacking, encourage hacking, or permit its use within their jurisdiction, and each variation comes with a different degree of state responsibility. [6]

The challenge of authoritative attribution to nation-state actors

Technical intelligence builds upon past incidents to create intrusion sets, or, the set of tools, infrastructure or tactics, techniques and procedures (TTPs) established during previous attacks that are grouped together and associated with a common actor. This process has some general standardization by convention and predictive success, but there is no one correct method. Accordingly, SANS in 2010 noted that:

> There is no rule of thumb or objective threshold to inform when linked intrusions should become a campaign. The best measure is results: if a set of indicators effectively predicts similar intrusions when observed in the future, then they have probably been selected properly. [7]

This predictive modeling creates important questions around the degrees of confidence regarding attribution, and how threat intelligence firms respond to novelty. Assuming an incident is correctly associated with an intrusion set, how is this intrusion set linked to a specific actor? Information like a common language, activity during specific hours, choice of targets, and the level of complexity of attack are often used to associate an incident group with a specific responsible threat actor. But this type of attribution extends beyond a purely technical association. The reuse of certain TTPs can complicate this attribution. For example, the vulnerability EternalBlue is reported to have been developed by the NSA but was later exploited by Russia, North Korea, and Iran. [8]

Brenden Kuerbis is a Postdoctoral Fellow at the Georgia Institute of Technology, School of Public Policy and a former Fellow in Internet Security Governance at the Citizen Lab, Munk School of Global Affairs, University of Toronto. His research focuses on the governance of Internet identifiers, and the intersection of cybersecurity with forms of Internet governance.

Models of attribution help digital forensics to structure collected intelligence and compare it to known intrusion sets. An example is the Diamond Model of Intrusion Analysis developed by Caltagirone and Pendergast. [9] The so-called "Q-model" developed by Thomas Rid and Ben Buchanan contains some excellent analysis of the problem of attribution although it is a graphic representation of the authors' ideas rather than a scientific model. [10] Both approaches, however, acknowledge the need for a nontechnical dimension to attribution. In the diamond model, the nontechnical dimension is described by the relationship between the victim and adversary. The strategic dimension of the Q-Model is described as a "function of what is at stake politically." [11]

While the political dimension of attribution might be quantified, it is necessarily relational, a product more of political science or intelligence studies than computer science. As sanctions or other disincentives are used to punish offensive cyber operations, we might expect cyber operations to adjust by taking steps to disguise their identity. The CIA's leaked Marble Framework, for example, has been described as providing the capability to change the language of the source code from English to another language like Russian or Farsi. [12] Meanwhile, cyber tools invented by one country are being reused by another. This suggests a technical race between forensic experts and counter-forensic obfuscation, but also an inequity of attribution based on state capability. Inequalities in attribution capabilities are said to have played a role in the breakdown of the United Nations (UN) Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. [13] While this obfuscation might serve powerful states well in the short term, it does little to mitigate the long-term damage of offensive cyber-attacks.

Farzaneh Badiei is a postdoctoral researcher at the Georgia Institute of Technology, School of Public Policy and the Executive Director of Internet Governance Project. She holds a Ph.D. in law and economics from Hamburg University Germany.

The attribution processes today

Preliminary research by Georgia Tech's Internet Governance Project has started to categorize the origin and characteristics of publicly attributed incidents. This work builds on the Council on Foreign Relations (CFR) dataset of state-sponsored cyber-incidents from 2005 to the present. [14] Reviewing 82 incidents identified by CFR between 2016 and the first quarter of 2018 (Table 1), we coded each case, identifying whether a state(s) and/or private actor(s) made a public attribution, as well as details related to the attribution including timing and outcome.

Actor type	Year			
	2016	2017	2018 IQ	Grand Total
No attribution made	6	5	1	12
Both government(s) and private actor(s)	4	3		7
Government(s)	7	7	1	15
Private actor(s)	12	26	10	48
Grand Total	**29**	**41**	**12**	**82**

Table 1. Incident attributions made by actor type

While publicly disclosed incident databases can be criticized as being just the tip of the iceberg, and two years of data based on a single dataset is certainly not conclusive, several interesting initial observations can be made. First, the vast majority of incidents (70, or 85%) resulted in some form of public attribution, with only 12 incidents (15%) not being attributed to a perpetrator. A small number of incidents, 7 (9%), were attributions involving both government(s) and private actor(s). These public attributions may have involved coordinated action between state and non-state actors (e.g., Wannacry), or attributions published by non-state actors citing anonymous government sources, or what appeared to be separate

attributions made independently (e.g., the Democratic National Committee hacks). Fifteen incidents (18%) were attributions made by government(s), including where identified government officials informally named alleged perpetrators, or formally accused them in official statements, reports, sanctions or indictments. The largest number of attributions have been made by private actors, a category that includes threat intelligence organizations, network security companies, and news media organizations. The importance of these actors in attribution is evident from the number of attributions made by them, which seems to be nearly doubling every year. It also highlights the need for a standardized attribution process.

The incident data also allow important distinctions to be made. Table 2 (below) shows attributions made to threat group(s) or state sponsor(s) by the actor type making the attribution. The total number of attributions made differs from the number of incidents (Table 1, previous page) as more than one entity in different actor types may be implicated per incident. Consistent with the incident observations above, private actors made substantially more attributions to both threat groups (31 versus 5) and state sponsors (38 versus 13) than did governments. Most attributions made by government(s) were made to a state sponsor. These attributions included the United States and allied countries accusing Iran, Russia and North Korea, as well as the United States implicating itself. As noted previously in Table 1 (previous page), governments made attributions in 15 incidents. Table 2 shows that governments attributed those incidents to state sponsors 13 times.

Governments (in this case, the US) attributed an attack to a threat group five times; in three of those times, the attribution was to both a threat group (APT28, APT 29, Lazarus) and an alleged state sponsor (Russia, North Korea). Only twice did a government (in this case, Switzerland) limit its accusation to a threat group (Turla), although a state sponsor was suspected. However, despite the appearance, a Chi-Square test concludes there is no significant difference between actor type regarding whom (threat group or state sponsor) they attribute incidents. Neither group is more likely, or perhaps better suited, to make attributions to a specific type of actor.

Attribution made by (actor type)	Incidents attributed to threat group	Incidents attributed to state sponsor
Both government(s) and private actor(s)	4	3
Government(s)	5	13
Private actor(s)	31	38
Grand Total	**40**	**58**

Table 2. Attributions made by actor type to actor type

New developments in advancing attribution technology

Within the private sector and academia, research into attribution technologies has advanced, with promising technologies set to significantly improve forensic confidence. New areas of research include Artificial Intelligence, monitoring campaigns from start to end, and improved monitoring of infrastructure. Our colleagues at Georgia Tech are investigating

attribution as part of the Rhamnousia project. [15] This project is connecting diverse datasets to fuel new algorithmic attribution methods which will speed up attribution. These and other research efforts will increase the speed, confidence, and breadth of potential attribution and represent dramatic improvements to digital forensics for their sponsors. But if individual states hoard this knowledge, they may not improve the general credibility of public attributions. Such military-funded efforts also raise questions about reproducibility (e.g., data collection) and the interaction with other legal and political attribution processes.

The need to develop legitimate attribution processes

While attribution technology is advancing, it does not and cannot eliminate the need for a legitimate process through which the technical attribution outcomes can be used to attribute an attack to a responsible party. Such a process has not been implemented, nor have the current processes been studied in detail. Attribution technologies focus on identifying specific machines and showing a pattern of behavior, not on identifying an organization or state. At some point, the evidence must be assessed and independently reviewed, and that cannot be carried out through technological means alone. Even with next-generation research on attribution, technology can only be used to establish technical attribution. The decision to blame a responsible party and impose sanctions on the identified attacker must take place through a nontechnical process.

States may conclude the attribution process by filing an indictment against the perceived offender or offenders. This state-led process may ultimately lead to the identified attackers and sanctions might be imposed on them. In the US, such indictments have usually been brought to a grand jury. [16] While some US-allied countries have welcomed such procedures, [17] a perception of a lack of due process could hamper the credibility of attribution more broadly. The proceedings of grand juries are not open to the public, and the accused are not given a chance to defend themselves nor to provide evidence. Should an attribution process punish the accused while their guilt remains unproven through the procedures of a domestic court? If attribution is to transcend a technical meaning to carry legal weight, how should the accused respond? Any attribution process will need to answer these questions.

Proposals for a Domestic Attribution Organization

While technology could transform attribution, so could organizational changes. International organizations like the European Union (EU) and North Atlantic Treaty Organization (NATO) have not fully integrated their members' cyber capabilities. Cyber attribution capability remains concentrated within a few nation states and distributed across many private sector actors, some of whom may be clients or contractors of nation-states. States have made efforts at the national level to undertake cyber attribution through bureaucratic and judicial processes without a global standard. In the US today, one of the last steps of this attribution process falls on the Secretary of Treasury's determination, in consultation with other cabinet officials, as to whether to freeze the actor's US-based assets.

The NSA's general counsel, Glenn Gerstell, has suggested revising the national cyber strategy to centralize the attribution function into a single agency, implying that the NSA could play a leading role. [18] While this might improve the current state of affairs, placing an attribution organization in a capable but secretive organization of a single nation-state would present unique challenges. While the NSA is a robust organization, it lacks an effective public affairs piece that impactfully manages disclosures or public communications. This aspect would help to inspire public confidence in its mission as well as trust from other countries.

Alternatively, Rosenzweig [19] and Shackelford [20] have proposed a National Cyber Safety Board in the US, something similar to an attribution organization that investigates the cause (e.g., network security flaws, human factors) and effects of an incident, and makes recommendations based upon findings. It is not explicitly performing attribution, although responsibility might be inferred from the findings. But this model is confined to the national level. The most interesting and challenging issues in attribution are international.

The proposed ***Cyber Deterrence and Response Act of 2018***, an attempt by the U.S. Congress to codify into law two Executive Orders (13694 and 13757) that focus on punishing foreign actors for significant malicious cyber-enabled activities, would place authority in the "President, acting through the Secretary of State," to determine which actors are engaged in, responsible for, or complicit in state-sponsored cyber activities. However, it leaves out any details about how this determination should occur. And here again, as an entirely unilateral initiative, the attributions made under this framework are unlikely to have global legitimacy. Even within the US, without a transparent process and evidence, attribution would be subject to question.

The US may be unique in having the number of independent agencies with cyber responsibilities. While the above proposals relate to organizational structure, perhaps the glaring absence from these plans is how results will be communicated. While the proposal for a National Cyber Safety Board implies it would produce a report, what would distinguish this from today's private sector produced threat intelligence reports?

These proposals suggest that the degree of centralization, transparency, checks and balances, and the importance of expertise are all critical questions in the attribution space. However, these domestic solutions are insufficient to address the global nature of cybersecurity attacks. Sanction mechanisms, domestic rules, and executive orders in one country will not be perceived as legitimate and neutral by third-party countries. This could reduce their willingness to participate in joint efforts, thereby allowing inter-state rivalries to limit collective action that would protect the Internet.

Proposals for a Transnational Attribution Institution

A Transnational Attribution Institution (TAI) could serve as a neutral global platform in which to perform authoritative public cyber-attributions. The TAI would be an independent entity or set of processes whose attribution decisions would aspire to be widely perceived as *unbiased, legitimate and valid*, even among parties who might be antagonistic (such as rival nation-states). Various proposals have been put forward with different scopes of activity, organizational structures, levels of stakeholder involvement, and evidentiary standards to potentially achieve such a process. Four of the leading attribution proposals use markedly different descriptions for this project. Microsoft describes their proposal as "a public-private forum to address attribution;" [21] the Atlantic Council called for a multilateral "attribution and adjudication council for cyber-attacks rising to the [legal] level of 'armed conflict'"; [22] a RAND study called for a "Global Cyber Attribution Consortium" of non-state actors; [23] a Russian think tank called for an "independent, international cyber court or arbitrage method that deals only with government-level cyber conflicts." [24]

The International Attribution Organization proposed in the Microsoft Digital Geneva Convention, and its subsequent articulation, [25] is one such proposal. This proposal included language suggesting that an independent attribution organization should 1) span the public and private sector while including civil society and academia 2) both investigate and serve an information sharing role and 3) resemble the International Atomic Energy Agency (IAEA). The initial proposal contained significant ambiguity as to whether this is describing a multi-stakeholder or multilateral model.

The Atlantic Council's 2014 *Confidence Building Measures in Cyberspace* report proposes a multilateral "attribution and adjudication council for cyber-attacks rising to the [legal] level of 'armed conflict'." [26] While the scope is only limited to incidents that rise above an international legal threshold, Healey et al., suggests that these assessments should result in the application of an enforcement mechanism. The organization, like the Digital Geneva Convention, draws on the IAEA for inspiration, but also the Biological Weapons Convention and Nuclear Nonproliferation Treaty.

RAND's *Stateless Attribution* report draws on both Atlantic Council's and Microsoft's work, but suggests that "an attribution organization should be managed and operated independently from states." Their report also differs from the Atlantic Council report in implying that an enforcement role is not needed. While the RAND Report classifies the Atlantic Council proposal as including non-state actors in collaborative investigations, this seems to confuse organizational management and support. As the Atlantic Council's proposal makes use of private sector data and expertise as a multilateral entity, the RAND proposal does not explain how non-state actors would assist targeted states without their involvement.

The Chernenko et al. paper presents an interesting contrast to the IAEA model for attribution. While not denying the significance of private sector actors, the Chernenko et al. proposal is explicitly state-based, recommending an "independent, international cyber court... that deals only with government-level cyber conflicts" [27] This scoping is smaller than the Microsoft proposal, but more inclusive than the Atlantic Council's, covering government-level cyber conflict which would include those below the threshold of armed conflict.

Each proposal offers different scopes of activity for a cyber attribution organization and pushes for dramatically different structures (e.g., multilateral vs. nongovernmental, or hierarchical vs. networked). And while the RAND Report [28] makes powerful arguments as to why states have conflicting incentives to participate in an attribution organization and cautions against their membership in any Consortium, none of the above proposals explicitly consider the incentives for private actors to participate in the forensic process. The Internet Governance Project (IGP) is tracking TAI proposals and critiquing their viability but believes more research is needed before a consensus can form.

Finally, a recent development highlights the growing demand for and stakes of neutral and widely accepted attribution. In late 2018, Mondelez International, Inc. filed a complaint against Zurich American Insurance Company. [29] In it, Mondelez sought relief for Zurich's alleged breach of its contractual obligations to Mondelez under an all-risk property insurance policy covering "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction ....". Zurich has asserted that the NotPetya attack, which caused damages more than $100M to Mondelez, was launched by a state-based actor and therefore excluded from the policy. Mondelez claims that Zurich bears the burden of proving the applicability of the exclusion. While numerous Western governments publicly accused the Russian government of launching NotPetya, Russia has steadfastly denied its responsibility. [30] However the court rules, it is unclear how the standard of proof will be met and what institution will provide it.

Challenges to proposed models (challenges of collective action in attribution)

Three major challenges are likely to present themselves in the creation of a transnational attribution institution; these include geopolitical conflict, building independent capability, and private sector participation. These challenges overlap with, but are more institutional than, the challenges of effective attribution and persuasive communication identified by the RAND study. Efficacy and communication will be contingent on the breadth of participation of public and private entities and their willingness to be transparent with the evidence. As with any political challenge, obtaining collective action from actors with competing interests presents a challenge.

Adversarial geopolitical relationships are likely to extend to any international forum. The advantage of such forums is that by joining the forum, the participants agree to adhere to the constitutive as well as procedural rules, even when they disagree over the particulars. The neutrality of international bodies is often established through the professionalism of participants: either technical independence as described in the RAND study or judicial independence might claim to embody this ethos. Should states as political actors be involved, as described by the Atlantic Council proposal, a majoritarian ethos might be needed to result in collective action. The consensus-based solution proposed in the Microsoft Digital Geneva Convention would undoubtedly face challenges.

In addition to the geopolitical challenges of managing an organization are those of creating trustworthy assessments. The Organisation for the Prohibition of Chemical Weapons (OPCW) manages to maintain global trust in its forensics with an independent laboratory, whose work it supplements with a network of over 20 certified laboratories [31] distributed across numerous national jurisdictions. The same strategy might help to supplement the capability of an attribution-based organization.

Finally, building this capability will require financial resources. Finding dedicated financial resources for a TAI would create its own set of challenges. Which country will agree to finance an organization tasked with rooting out its espionage operations? What incentives are there for the private sector? The cyberspace domain is uniquely defined by private sector participation and ownership of the core infrastructure. In this respect, Microsoft's Digital Geneva Convention was served well by including the private sector, but this thrust was undermined by the way it drew upon the model of the International Atomic Energy Agency. Was Microsoft proposing an independent, member state-funded international organization, like that of the IAEA? Or by empowering the "the private sector, academia and civil society," [32] was it suggesting a multi-stakeholder model? At face value, it appears that governments will set the rules, while private actors will lend their services and data, but nothing is stated about how these interests might be aligned. If a subset of private sector cybersecurity firms has advanced forensic capability equaling or exceeding that of most states, why would they participate in a monopsony attribution organization? Presumably, they would have to be compensated. Alternatively, if access to the Internet's infrastructure allows an investigation to backtrack the origins of an attacker, what process should enable the acquisition of relevant evidence? Should this layer of attribution include partnerships with national law enforcement or permit international inspections? Either way, this potentially burdens the private sector and has implications for global privacy.

Research agenda going forward

At present, threat intelligence firms and national security agencies are the primary producers of cyber forensics and attribution. While ideal models for attribution and novel policy proposals were described above, too little is known about the current state of affairs. Modeling of state(s) behavior in attribution should also incorporate the role of private actors. [33] A research agenda going forward should attempt to better understand the process of attribution, and, based on empirical research and the current state of attribution, provide novel institutional designs and processes that go beyond merely replicating the existing international organizations. This might include exploring research questions like:

- How effective is attribution at initiating an international response?
- How do the public and state responses to an attribution differ based on whether the forensic assessment comes from the private sector, state intelligence, law enforcement, or second-hand media reporting?
    - Are there different accepted levels of confidence?
    - How does the level of public transparency differ?
- How do geopolitical rivalries undermine the confidence placed in attribution?
- Is a hierarchically-organized institution really needed to align participant incentives, or can a more loosely organized form of networked governance or market satisfice?
- How would different visions for attribution address the concerns of stakeholders, distribute costs, and gain momentum?

With a better understanding of the present state of attribution, we can better seek to define governance-based solutions. This paper has described several competing visions for an attribution-based organization. Without greater clarity on the trade-offs inherent to each, political capital might be saved and more efficiently directed at a workable solution.

IGP will continue to explore these questions and seek a better understanding of how governance models might help build global trust in forensic evidence so that responsible parties can be held accountable. Despite the capacity of advanced threat actors, the need to protect intelligence sources and methods, and conflicting nationalistic biases, we believe that global consensus is possible.

REFERENCES

Burgess,M. "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files," Wired Magazine (blog), May 7,2017, https://www.wired.co.uk/article/cia-files-wikileaks-vault-7.

Caltagirone, S. Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis," May 7, 2013, 61.

Charney, S et al. "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Corporation, June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

Charney, S "Cybersecurity Norms for Nation-States and the Global ICT Industry," Microsoft on the Issues (blog), June 23, 2016, https://blogs.microsoft.com/on-theissues/

2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/.

Chernenko, E., Demidov, O., and Lukyanov, F. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," Council on Foreign Relations (blog), February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-andadapting-cyber-norms.

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M.S. (2017). *Stateless Attribution.* RAND Corporation.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America, 114*(11), 2825–2830, http://doi.org/10.1073/pnas.1700442114

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015, July). Cyber Intrusion into US Office of Personnel Management: In Brief. Congressional Research Service, https://fas.org/sgp/crs/natsec/R44111.pdf.

Gerstell, G. "How We Need to Prepare for a Global Cyber Pandemic" (April 9, 2018), https://www.nsa.gov/news-features/speeches-testimonies/speeches/09Apr2018-gerstell-cyberpandemic.shtml.

Healey, J ed., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013).

Healey, J et al., "Confidence-Building Measures in Cyberspace: A Multiskeholder Approach for Stability and Security" (Washington, D.C.: Atlantic Council, November 2014), http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

Internet Governance Project, "Defusing the Cybersecurity Dilemma Game through Attribution and Network Monitoring.", blog, April 13, 2018, https://www.internetgovernance.org/2018/04/13/defusing-cybersecurity-dilemma-gameattribution-network-monitoring/.

Lee R. "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks." SANS DFIR (blog), March 4, 2016. https://digital-forensics.sans.org/blog/2016/03/04/the-problems-withseeking-and-avoiding-true-attribution-to-cyber-attacks/.

Lin H, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 2, 2016), https://papers.ssrn.com/abstract=2835719.

Rid., T and Buchanan., B. "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1–2 (January 2, 2015), 4–37, https://doi.org/10.1080/01402390.2014.977382.

Rep. Ted Yoho, "Cyber Deterrence and Response Act of 2018," H.R. 5576 § (2018), https://www.congress.gov/bill/115th-congress/house-bill/5576/text.

Rosenzweig, P. "The NTSB as a Model for Cybersecurity," R Street Shorts (R Street, May 9, 2018), https://www.rstreet.org/2018/05/09/the-ntsb-as-a-model-for-cybersecurity/.

Michael Schmitt, & Liis Vihul. (2017). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, retrieved August 17, 2018, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advancecyber-norms/.

Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.

Security Intelligence, Defining APT Campaigns (2010) https://digitalforensics. sans.org/blog/2010/06/21/security-intelligence-knowing-enemy

Segal, A,. "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat." Council on Foreign Relations (blog), June 19, 2018, https://www.cfr.org/blog/theft-and-reuseadvanced-offensive-cyber-weapons-pose-growing-threat.

Segal, A., Grigsby, A., "New Entries in the CFR Cyber Operations Tracker: Q1 2018," Council on Foreign Relations, April 23, 2018, https://www.cfr.org/blog/new-entries-cfr-cyber-operationstracker-q1-2018.

Toon, J. "$17 Million Contract Will Help Establish Science of Cyber Attribution," Georgia Tech Research, Horizons (blog), November 29, 2016, http://www.rh.gatech.edu/news/584327/17-million-contract-will-help-establish-science-cyber-attribution.

Volz, D, & Sarah Young. 2018, "White House Blames Russia for 'reckless' NotPetya Cyber Attack." *Reuters.* https://www.reuters.com/article/us-britain-russia-cyber-usa/white-houseblames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.

Wittes, B, "Mandiant Report on 'APT1,'" Lawfare (blog), February 20, 2013, https://www.lawfareblog.com/mandiant-report-apt1.

NOTES

1. "Cyber Intrusion into U.S. Office of Personnel Management: In Brief" (Washington D.C.: Con-gressional Research Service, July 17, 2015), https://fas.org/sgp/crs/natsec/R44111.pdf.
2. Ibid.
3. Robert M. Lee. "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks." *SANS DFIR* (blog), March 4, 2016.
4. Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 2, 2016).
5. Benjamin Wittes, "Mandiant Report on 'APT1,'" *Lawfare* (blog), February 20, 2013.
6. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace*, 1986 to 2012 (Vienna, VA: Cyber Conflict Studies Association, 2013).
7. Security Intelligence, Defining APT Campaigns. SANS blog, June 21, 2010.
8. Adam Segal. "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat." *Council on Foreign Relations* (blog), June 19, 2018.
9. Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intru-sion Analysis," May 7, 2013, 61.
10. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015), 4–37.
11. *Ibid.*
12. Matt Burgess, "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files," *Wired Magazine* (blog), May 7, 2017.
13. Michael Schmitt, & Liis Vihul. (2017). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, retrieved August 17, 2018, https://www.justsecurity.org/42768/international-cyber-lawpoliticized-gges-fail-ure-advance-cyber-norms/.
14. Adam Segal and Alex Grigsby, "New Entries in the CFR Cyber Operations Tracker: Q1 2018," Council on Foreign Rela-tions, April 23, 2018. The Council on Foreign Relations is not the only entity collecting and publishing cyber-incident data. Another example is the Dyadic Cyber Incident and Dispute Dataset by Valeriano and Maness (2015), as well as incident data collected by the New America Foundation. Methodological questions can be raised where differences occur be-tween these datasets, e.g., in what is considered a state-sponsored "incident", or an attribution to a specific perpetrator.
15. John Toon, "$17 Million Contract Will Help Establish Science of Cyber Attribution," *Georgia Tech Research, Horizons* (blog), November 29, 2016.
16. As indictments are filed as felony charges at the federal level, it has to be argued in front of a grand jury. For a specific indict-ment on hackers which took place through a grand jury process, see these documents.
17. For example after the US Department of Justice indicted attributed a set of cyberattacks to Iranian hackers, backed by the Iranian revolutionary guard, the UK issued a statement supporting the US efforts in carrying out attribution.
18. Glenn S. Gerstell, "How We Need to Prepare for a Global Cyber Pandemic," NSA news release (April 9, 2018).
19. Paul Rosenzweig, "The NTSB as a Model for Cybersecurity," R Street Shorts (May 9, 2018).
20. Shackelford, Scott, and Austin Brady, "Is It Time for a National Cybersecurity Safety Board?" *Albany Law Journal of Science and Technology*, January 12, 2018.
21. Scott Charney, "Cybersecurity Norms for Nation-States and the Global ICT Industry," *Microsoft on the Issues* (blog), June 23, 2016.
22. Jason Healey et al., "Confidence-Building Measures in Cyberspace: A Multiskeholder Approach for Stability and Security" (Washington, D.C.: Atlantic Council, November 2014).
23. John Davis et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation, 2017), https://doi.org/10.7249/RR2081.
24. Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations* (blog), February 23, 2018.
25. Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Cor-poration, June 2016).
26. Healey, note 21 above.

NOTES

27. Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms."
28. Davis et al., *Stateless Attribution.*
29. Mondelez International Inc. v Zurich American Insurance Company. No. 2018L011008. Circuit Court of Illinois, October 10, 2018.
30. Volz, Dustin and Sarah Young. February 15, 2018. "White House Blames Russia for 'reckless' NotPetya Cyber Attack." *Reuters,* https://www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-forreckless-notpetya-cyber-attack-idUSKCN1FZ2UJ.
31. "Lab Receives OPCW Recertification." *Lawrence Livermore National Laboratory* (blog), Feb-ruary 8, 2013, https://www.llnl.gov/news/lab-receives-opcw-recertification.
32. Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms" (Microsoft Corporation, June 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.
33. Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, at-tribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America, 114*(11), 2825–2830. http://doi.org/10.1073/pnas.1700442114.

THE CYBER DEFENSE REVIEW

RESEARCH NOTE

Modelling the Cognitive Work of Cyber Protection Teams

Colonel Stoney Trent
Dr. Robert R. Hoffman
Lieutenant Colonel David Merritt
Captain Sarah Smith

ABSTRACT

Cyber Protection Teams (CPTs) defend our Nation's critical military networks. While Cyber Security Service Providers are responsible for the continuous monitoring and vulnerability patching of networks, CPTs perform threat-oriented missions to defeat adversaries within and through cyberspace. The research we report here provides a descriptive workflow of cyber defense in CPTs as well as a prescriptive work model that all CPTs should be capable of executing. This paper describes how these models were developed and used to assess technologies and performance of CPTs. Such models offer a variety of benefits to practitioner and research communities, particularly when the domain of practice is closed to most researchers. This project demonstrates the need for continual curation of CPT work models as well as the need for models of work for the other types of cyber teams (i.e. Mission and Support) in the Cyber Mission Force.

INTRODUCTION

Cyber Protection Teams (CPTs) defend our Nation's critical military networks. While Cyber Security Service Providers are responsible for the continuous monitoring and vulnerability patching of particular networks, CPTs perform threat-oriented missions to defeat adversaries within and through cyberspace. Each 39-person CPT must be able to work with network security teams and other CPTs to counter cyber threat actors. When fully operational, the Cyber Mission Force will include 68 CPTs, which will be manned, trained and equipped by the Military Service Departments. [1] Within the Cyber Mission Force, CPTs are allocated to an operational command and aligned with one

Stoney Trent is a Cognitive Engineer and Army Cyber Warfare Officer, currently serving as a U.S. Army War College Fellow at the National Security Agency. Previously he served as the Chief of Experimentation and Director of the Cyber Immersion Laboratory at U.S. Cyber Command. He has 22 years of experience in operations and intelligence assignments in tactical, operational and strategic echelons. His research has focused on team cognition in mission command, intelligence and cyberspace operations. His current work is focused on improving technology innovation for cyberspace operations.

of four mission areas: Combatant Command (CCMD), Service Department (Army, Navy, Air Force, and Marine Corps), Department of Defense Information Network (DODIN), and National Threats. To maximize flexibility, these teams must be able to perform reliably as well as be interchangeable and interoperable.

CPTs must be able to perform three basic types of missions. [2]

1. Survey: Short duration assessments that provide the supported organization with recommended mitigations based on an assessment of network vulnerabilities.
2. Secure: Harden and defend cyber key terrain; and
3. Protect: Time-sensitive deployments that include Survey and Secure tasks, but also include helping an organization recover from the effects of a cyber intrusion.

The research we report here provides a descriptive workflow of cyber defense in CPTs as well as a prescriptive work model that all CPTs should be capable of executing.

Work models, such as the one described here, provide a foundation for improvements to work processes. As an illustration of required or desired workflows, work models provide a bridge to common ground between researchers and practitioners, particularly when the work domain is difficult to access, or is esoteric. The model in this report has multiple purposes. The first purpose is to inform the design of experiments to assess current and emerging technologies for operational fit. The second is to educate developers, who may have limited knowledge of CPT work, about the tasks that require technical support. The third is to inform revisions to operational doctrine. Finally, this model is meant to provide the basis for operational and strategic planning of defensive cyberspace operations.

David Merritt is the Experimentation Branch Chief at U.S. Cyber Command, where he leads capability assessments and experiments to bridge the gap between research and operations. David's interest in human-system cyber issues stems from his previous experience leading the incident response efforts of the Air Force Computer Emergency Response Team, as well as his Ph.D. research on leveraging a mix of expertise between humans and machine learning agents.

Developing the model

To develop an initial model of CPT work, the research team started with a review of the literature, including doctrine, published reports, and conference proceedings. Prior research on defensive cyber work had established multiple workflow models. [3][4][5] One of these models was aimed at the development of a computer simulation of the work process of cyber incident response teams. [6] Reed and colleagues worked with cyber analysts at the Sandia National Laboratories to develop and implement a workflow model (using the ACT-R computational cognitive model). The workflow model they developed was similar in many respects to another workflow model developed at U.S. Cyber Command. [7] These prior models described defensive cyber work at a very high level of primary tasks (e.g. Review Alerts, Evaluate Risk, Understand, Engage Mitigation).

Beginning with these models, we created an initial model with the benefit of a former CPT member who is a co-author of this paper (SJS). Our initial model is presented in Figure 1. For the model to satisfy our purposes, we needed to elaborate and validate it with input and suggestions from CPT members from all the various Mission Types previously mentioned. To do so, we interviewed current team members from across the Cyber Mission Force.

The research team solicited 50 volunteer interviewees from 19 CPTs. Army (8 CPTs), Air Force (3 CPTs), Navy (4 CPTs) and Marine Corps (4 CPTs) representing DODIN, National, CCMD, and Service mission areas. As individuals and as teams, participants had a range of experience in addition to their foundational cyber training. Some had participated in exercises but had not yet been on actual missions. Most had some background in computer or information science; some had experience in information security.

Robert R. Hoffman received his Ph.D. in experimental psychology from the University of Cincinnati. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a Fellow of the Association for Psychological Science, a Fellow of the Human Factors and Ergonomics Society, a Senior Member of the Association for the Advancement of Artificial Intelligence, and a Fulbright Scholar. He has been recognized internationally for his research on the psychology of expertise, the methodology of cognitive task analysis, and the issues for the design of complex cognitive work systems, including cyber work systems.

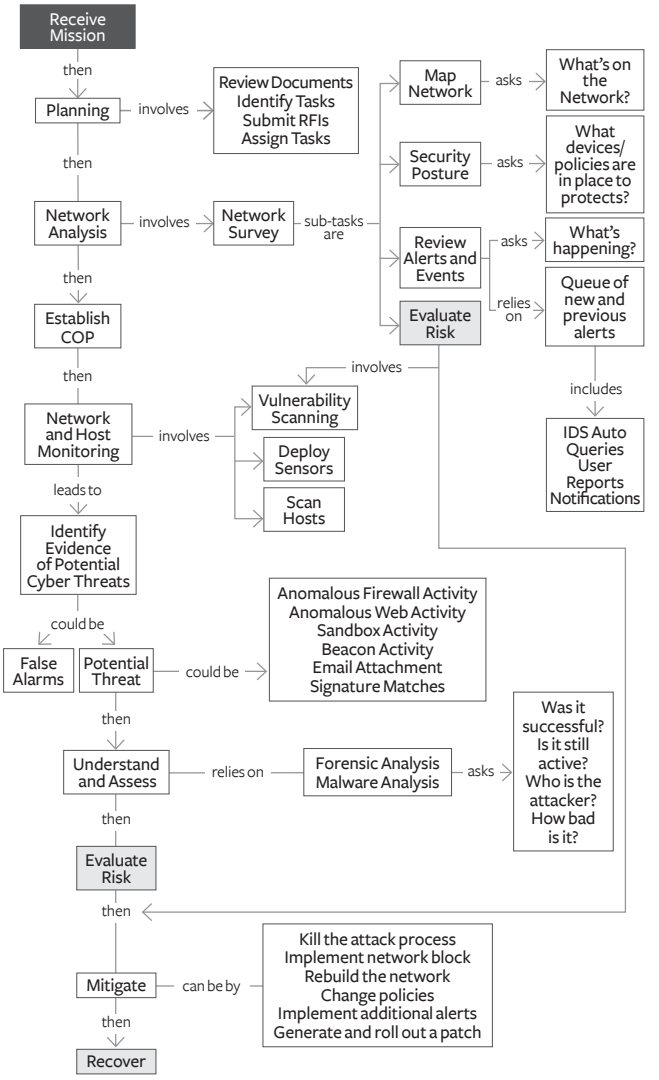


Figure 1. Initial Workflow model

On the other hand, some entered the CPT community with little to no computer science background. Embracing such diversity was necessary for the interview results and for the refined work model to reflect the variability of experience in actual practice.

In the interviews, the participants were shown a diagrammatic model of the work. As the participants

Sarah Smith is a Capability Analyst at U.S. Cyber Command, who supports experimental activities designed to understand operations and inform technical solutions. Prior to her assignment at U.S. Cyber Command, Sarah served as a Cyber Network Defense (CND) Manager for a Cyber Protection Team (CPT).

recounted their experiences, they referenced the diagram and provided annotations and suggestions for how it could be corrected, improved, and refined. The first interviews began with the model presented in Figure 1. Interviews were conducted over two months, at multiple locations, and the workflow model was successively iterated and refined. As the interviewing continued, fewer and fewer modifications were proposed. The diagram converged on a consensus model, acknowledged by multiple independent CPT members as being a good depiction of their workflow, regardless of CPT Service or Mission alignment.

Notice that the left-hand side of Figure 1 is a sequence of events or activities. Many work models assume that work can, and should, be represented as a series of clear-cut steps or stages. As our research continued to refine the model, however, it was discovered that the work of CPTs needs to be described in terms of parallel tasks and feedback loops, not as a series of steps or stages. Figure 2 presents a "high-level" overview of the workflow model. The purpose of this high-level overview is to offer critical work task elements without the potentially overwhelming details about the sub-tasks. (In comparison to planning models for full missions, the diagrams created for CPT modeling are elementary.

At the top and bottom of Figure 2 are two continuous horizontal lines. The line at the top highlights the fact that CPT interaction with intelligence, and with the supported organization (circles at the left side of the Figure) are continuous processes that occur at many points throughout a mission. The line at the bottom serves as a reminder that CPT members remain cognizant of potential vulnerabilities or threats and the evaluation of risks. The full model expands on the concepts and activities that are involved for each of the major nodes that are highlighted in green

in Figure 2: Planning and Logistics, Monitoring and Collecting, Sensemaking, and Closure. The full model is presented in Figure 3.

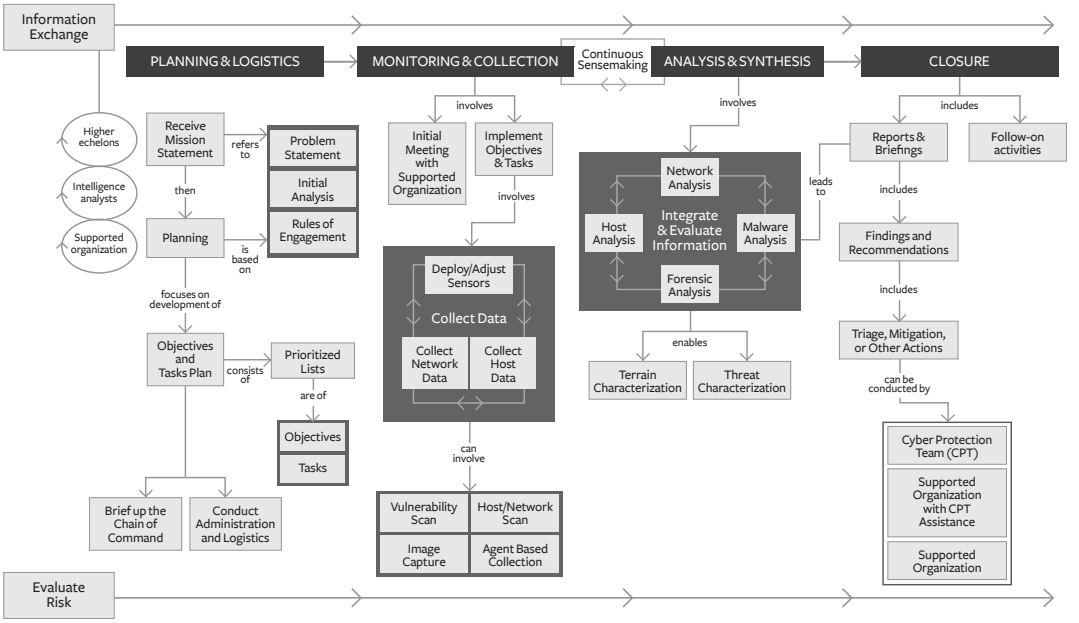


Figure 2. Abstract view of CPT workflow

From the standpoint of cognitive work analysis, a few features of the model are noteworthy. First, the model does not match the current doctrine in all respects. The primary tasks described in earlier models and in CPT CONOPS involve stages of Survey, Secure, Protect, and Recover. This and other aspects of CPT doctrine are still evolving. The field study interviews revealed that there is much more to CPT mission-related activity. Specifically, the primary activity categories are perhaps better described as Planning, Collection, Analysis and Synthesis, and Closure. Within each of these are many sub-tasks and activities.

Second, while CPT work can be understood as having stage-like primary activities, it is not possible to capture the range and details of CPT mission-related activities in a step-wise, sequential or linear chain model. The initial model was built upon a sequential "backbone," as pointed out above (Figure 1). Some CPT activities are sequential, and a high-level sequence can be discerned in a retrospective study of any given cyber mission, but from the field study interviews, we learned that most CPT activities are interdependent (note the cross-links in Figure 3). Some activities are cyclical, some are continuous, and others are parallel. For example, the process of creating an accurate logical-physical map of the cyber-terrain involves waves of iteration and refinement as different subtasks are conducted (e.g. passive scan, active scan, host monitoring, etc.). Thus, sub-tasks that occur in cycles were represented as cycles in the diagram, and some of these are nested. For example, high-level sensemaking

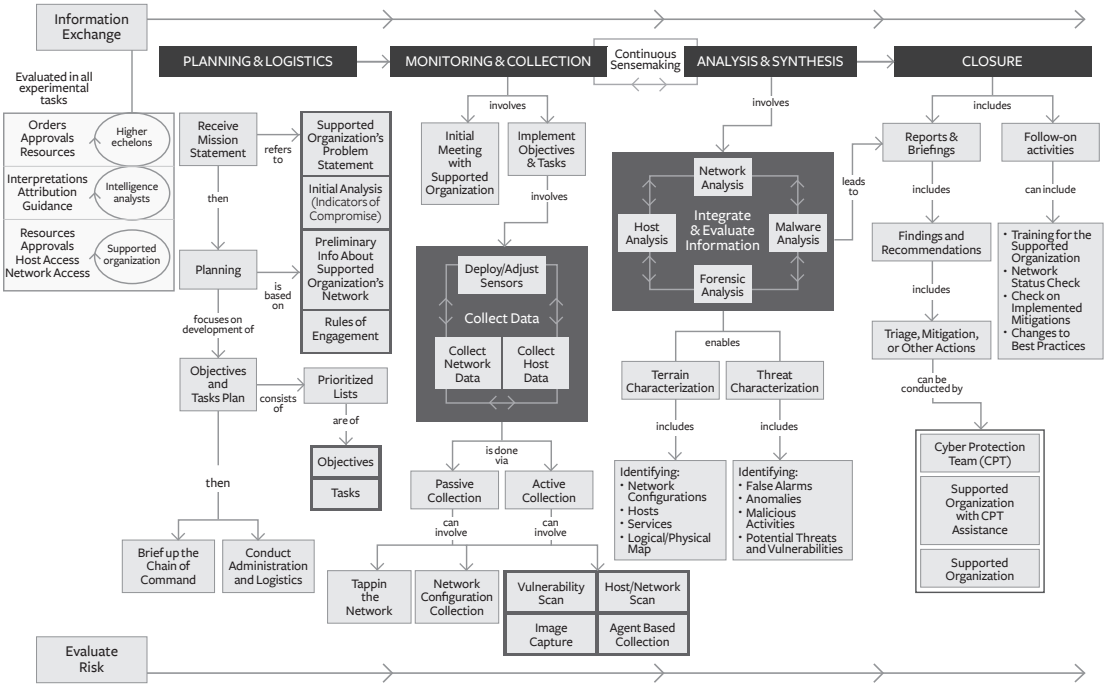


Figure 3. Detailed CPT work model

is represented by the cycle between Monitoring/Collection and Analysis/Synthesis. Within Monitoring/Collection is an embedded cycle of Sensor Deployment, Traffic Monitoring, and Host Monitoring.

It is important to note that this model represents the collection of tasks that may be considered ideally rigorous. As such, this model represents how an experienced team would perform a mission without time constraints. In fact, no team performs all these tasks for all missions. Instead, teams leverage their understanding of the situation to adapt their work to suit the constraints and intent of the mission and taking into account the mission of the network owner (i.e. mission essential elements of the network). As a model of ideally rigorous CPT work, it illustrates the breadth of work that CPTs must be able to perform and therefore helps to describe technology support requirements.

Putting the model to work

An important reason for including all the fine grain detail (Figure 3), rather than reducing the complexity to a simpler representation, is that in expressing the full range of the tasks that CPTs conduct, one can create "layers" that represent different Mission types, or Services differences. This contextualizes the differences by expressing them within the broader context. Figure 4 presents a layer (green coloration) of what is involved in the Network Mapping

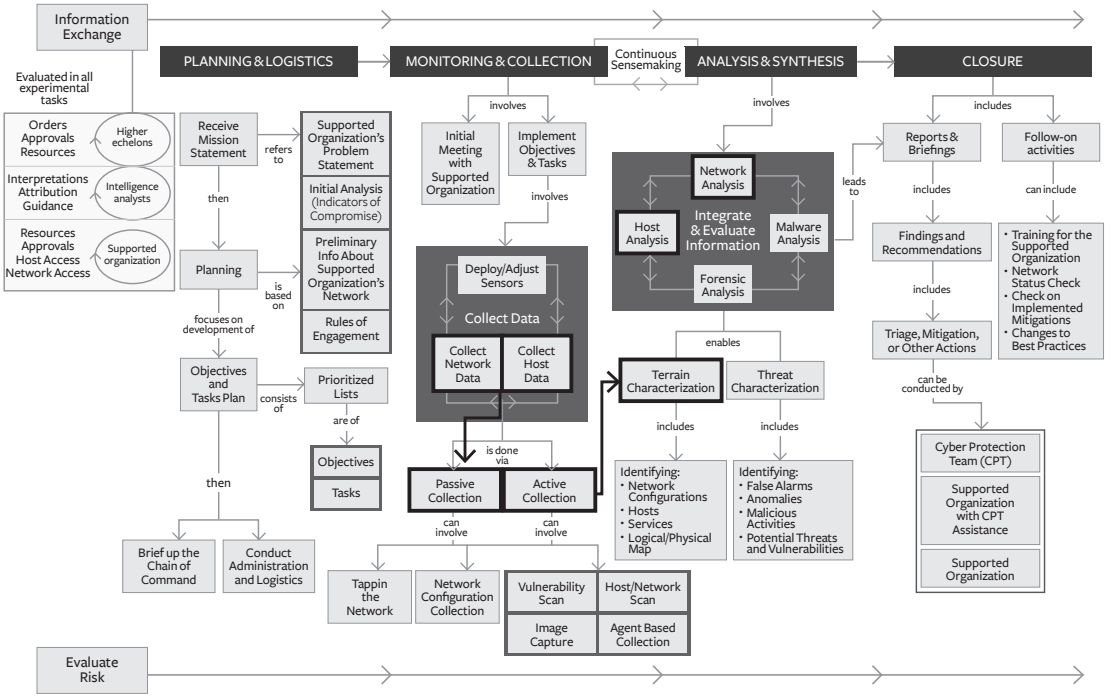


Figure 4. CPT work model overlaid with network mapping task

Task. Figure 5 shows a layer (orange coloration) that depicts what is involved in the Malware Identification task.

Workflow models of this kind have several immediate uses, described above, but going forward, they have additional applications that can be of value to the Cyber Mission Force and researchers who are developing technologies for the Force.

- Such a task decomposition can be reviewed to identify aspects of CPT performance that can be readily observed and measured.
- Because CPT work is distributed across many work roles, this work model can be used to document which roles are involved with which particular tasks.
- Workflow models can be used in a "checklist" mode to track performance and CPT qualifications.
- Workflow models can be used in training and can allow individuals who are less familiar with CPT work to come to an understanding at levels of detail.
- While CPT work is heavily dependent on computational technology, it is fundamentally cognitive work. Workflow Models can be used to highlight CPT activities and functions that can only be conducted by human decision makers. This highlights the importance of training to high levels of proficiency and expertise.

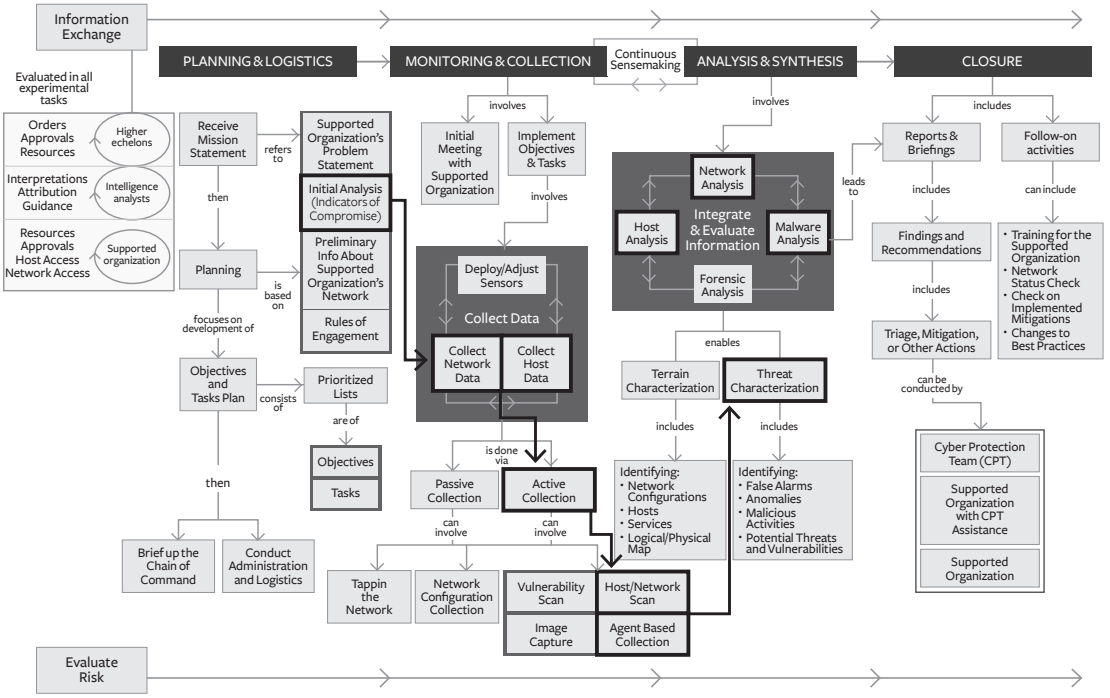


Figure 5. CPT work model overlaid with sensor deployment task

- Workflow models reveal work design issues, such as bottlenecks and capability gaps.
- Workflow models provide a focus for discussion of work methods, desired tool functionalities, and best (and sub-optimal) practices.
- Workflow models allow representation and comparison of mission differences, Service differences, down to the level of individual CPTs.
- Workflow models can be used to identify aspects of the work that demand additional or better technical support.
- Workflow models inform CONOPS and allow tracking of changes in CONOPS. At an even higher level, workflow models provide a window on the current work that can inform and contextualize the design of entire campaigns of experimentation.

Currently, CPT work methods are evolving, and technology support requirements are continuing to emerge. Thus, the workflow model presented here represents the state of CPT work methods as they currently exist within the CMF. Cyber work methods and technologies are evolving at a pace which demands continual curating of this "as-is" model. Furthermore, this project demonstrates the need for models of work for the other types of cyber teams (i.e. Mission and Support) in the CMF. Although our research team used methods that are typical

for field studies in other work domains, the research team found that automated instrumentation might provide data for mathematical models of cyber teamwork. Such mathematical models should prove invaluable for simulations to aid with operational and strategic planning. Our current research is pursuing this notion.

DISCLAIMER

This paper reflects the views of the authors. It does not represent the official policy or position of Department of Defense, U.S. Cyber Command or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

ACKNOWLEDGMENT

The authors would like to acknowledge the contributions to the research reported here by the Applied Physics Laboratory, Johns Hopkins University.

NOTES

1. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
2. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
3. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
4. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
5. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
6. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
7. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

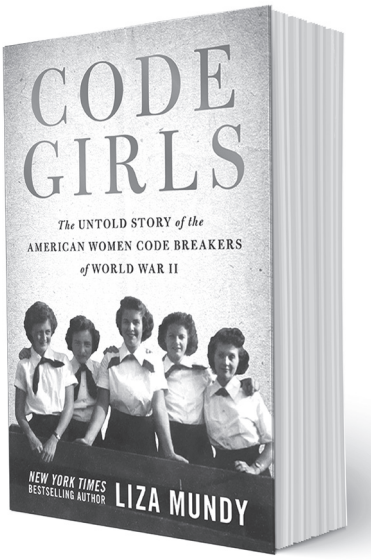
The Cyber Defense Review

BOOK REVIEW

Code Girls: The Untold Story of the American Women Code Breakers of World War II

by Liza Mundy

Reviewed by
Courtney Gordon-Tennant



EXECUTIVE SUMMARY

In *Code Girls*, Liza Mundy explores the previously untold story, and largely unrecognized contributions, of the first women to officially serve as part of World War II US intelligence code-breaking efforts. At approximately 11,000, these women comprised more than fifty percent of the 20,000 workers. Based on voluminous research from the National Cryptologic Museum and the National Archives, Mundy brings to life these civilian and military women's stories as they decrypted messages from the enemy Axis Powers, thereby significantly advancing the Allied war effort. Meticulously researched, this work provides fascinating insights for all who have an interest in women's contributions and progress within the military as well as mathematics and computing professions. Historians, intelligence and cyber professionals, and feminists should find it especially illuminating. Mundy paints a vibrant picture of the challenges faced by the Allies as well as the workplace, living conditions, personal stories and struggles experienced by these women code-breakers executing their classified mission. This book does not extensively cover the methods and techniques of code-breaking; instead, the author wonderfully combines personal firsthand stories from these women's lives with the significant impact their sacrifice and efforts had on strategic intelligence supporting military operations, thereby turning the tide of a seemingly unwinnable war into ultimate victory. Similar to the style of popular movie/book *Hidden Figures* in describing African American women's contributions to the Space Race, *Code Girls* brings to light the substantial contributions women made in Intelligence gathering during World War II.

Courtney Gordon-Tennant is the Army Cyber Institute (ACI) staff attorney. She earned her Bachelor of Arts in Political Science from Barnard, her Juris Doctor from Brooklyn Law School, and her Tax LLM from the University of Alabama, and is admitted to the Connecticut and New York bars. Courtney began her career as a legal assistant at Epstein, Becker & Green in NYC. During law school, she commissioned in the Navy Judge Advocate General's (JAG) Corps in 2008. As a Navy JAG, she has served as an Assistant Staff Judge Advocate (SJA) (in-house counsel), prosecutor, a legal assistance attorney, defense counsel, formal physical evaluation board counsel for Navy and Marine clients, and legal observer-trainer. She deployed to Djibouti, serving as the Camp Lemonnier SJA and Guantanamo, serving as the Joint Task Force Guantanamo International Committee of the Red Cross (ICRC) Liaison and Freedom of Information Act (FOIA) Officer. Personal accomplishments include several marathons, half-marathons, and distance swims.

REVIEW

Recalling the pervasive operational security (OPSEC) initiatives during World War II, such as "Loose Lips Sink Ships" or "Somebody Talked," it is not difficult to ascertain why the stories of approximately eleven thousand female code-breakers were mostly left out of history books. Those who served were strongly encouraged to maintain OPSEC, and the US government itself was slow to declassify the salient details until the 1990s. The author pieces together a compelling and coherent narrative from thousands of boxes of records, rosters, memos, declassified reviews, and other documents. She also convinced about twenty of the women to relate their personal stories. If this research had started earlier, more of these primary sources would have been available to provide commentary, although perhaps not all would have been willing.

As an increasing number of men were sent to the European and Pacific theaters, Mundy describes how recruiters lobbied intensely at the Seven Sisters' Schools, pulling on the patriotic heartstrings of the women to convince them to serve. As many had ties to the war through their husbands or boyfriends, fathers, brothers, cousins, friends, and neighbors, this was not a tough sell for recruiters who did not even disclose the nature of the classified mission. Consistent with other World War II writing, this book emphasizes that this was everyone's war, and all had a role to play.

The first code-breaking recruits were brought into the Army and Navy as civilians. Their numbers would grow from the low hundreds on the eve of Pearl Harbor, to about 7,000 in the Army and 4,000 in the Navy in 1945. For many, this was their first paid employment. The work was not glamorous, and men were not eager to fill these roles. Nonetheless, the women were screened to see if they had sufficient grit to handle

the demanding assignment. Aptitude tests rated them as clerical, technical, or analytic. Those that scored the highest were rated as analytic and would serve in a code-breaking assignment. Code-breakers worked three shifts: day (8am-4pm), swing (4pm-12am), and graveyard (12am-8am). In contrast to a traditional military hierarchy, the Arlington post, where much of the code-breaking was performed, was a largely flat operation that encouraged decision-making inputs from the female code-breakers.

Despite the propaganda, the war was not going well during the early days, and code-breakers were learning their trade as they went. Readers of this book may not necessarily walk away understanding how code-breaking worked, but Mundy emphasizes that success in the assignment required a greater memory than today. The tasks, comparing and recognizing patterns, provided much more of a mental challenge with the absence of modern computers, artificial intelligence, or electronic devices to assist with the tasks.

One example of these pioneers was Agnes Driscoll, who was a young mathematics teacher initially recruited to be a stenographer. After being transferred to the Navy's postal and censorship office, she began to methodically decode messages of the Japanese fleet code throughout the 1920s and 1930s. She eventually became such an expert that she taught code-breaking to men, who then received approximately twenty-five to thirty percent higher compensation. For example, a 1941 Navy memo proposed paying female clerks, typists, and stenographers $1,440 per year, while men in these positions were to be paid $1,620. For Ph.D's, the gender-gap heightened as females were paid $ 2,300 compared with $3,200 for males. Because it was not yet illegal (through the Civil Rights Equal Pay Act of 1964) to provide "Equal Pay for Equal Work," female code-breakers were paid less than men for the same tasks. Another unsung example from Mundy's work is Elizabeth Smith Friedman, a veteran code-breaker since 1927 whose codes would be used by the Office of Strategic Services (OSS), the predecessor to the Central Intelligence Agency (CIA). As there was not a way to correct the record without running afoul of OPSEC and risking treason, her husband, William Friedman, an Army code breaker is sometimes incorrectly credited for her efforts, although she was the one who introduced him to the craft.

Despite their skills and work ethic, the author asserts these women were often treated with condescension and harassment instead of respect. While both the Army and Navy were looking for women with backgrounds in science, math, music, and language, Mundy shows some stark differences between the service's treatment of women. The former allowed women to serve overseas and welcomed non-whites were into the code-breaking operation. In the latter, more code-breakers would serve in uniform than in a civilian status, restricted women to domestic service, and avoided bringing African-American women into their operations. Nonetheless, at the war's conclusion, almost all women were discharged or resigned. Women with families were traditionally supposed to stay home, supported by their husbands; despite their experience, that cultural viewpoint remained stalwart. Agnes Driscoll was one of the few that kept serving after the war.

One interesting anecdote from *Code Girls* hints at OPSEC's impact on daily life. It is widely acknowledged that everyone was called upon to support and sacrifice to further the war effort. In stark contrast to today's society, the public was encouraged to transport those in uniform. In doing so, they would inquire about the servicemember's duties. It was impressed upon the women that if anyone should ask, they were to discourage further engagement on the issue by answering that they were doing clerical work, sharpening pencils, or filling ink blots. In one instance, unbeknownst to the code-breaking WAVE, a Navy Admiral in civilian clothes was the one inquiring; when she answered, "clerical work," the Admiral gave her a wink, wordlessly conveying that she passed the secrecy test. OPSEC had been maintained!

As in other wars and conflicts, Mundy links the intelligence gathered by the code-breakers to the critical turning points in several battles, thereby changing the eventual outcome of a seemingly desperate war. This intelligence information included enemy supply status, troop training, promotions, convoys sailing, reserves, attacks, changes in the makeup of the Japanese Army, railroad conditions, shipboard losses, casualties, convoys delayed, tools lost, and plans to hamper US air activity. At that time, ships were utilized as the primary form of transport, and they carried troops, food, and medicine as well as spare parts for aircraft and weapons. Code-breaking information about these itineraries revealed to the US what enemy ships needed refueling, what ships were in a given harbor, what convoys were deploying and their likely destination. This intelligence made its way to the highest levels of the US military, to Admiral Chester Nimitz in the Battle of the Coral Sea and the Battle of Midway in 1942, and General Douglas MacArthur in Operation Cartwheel in 1943, to a deception campaign that successfully diverted the German military away from the correct landing sites in France for D-Day in 1944. The codebreakers' intelligence reduced US casualties and expedited destruction of the Axis powers infrastructure.

One of the book's greatest strengths is its snapshot into the daily lives of women code-breakers. Recruits, who often joined due to patriotism, learned the stark difference from the glossy recruiting advertisements when they arrived in Washington, D.C. (pre-air conditioning) for their shifts with clean dresses, and departed with their clothes stuck to them from the intense humidity. Generally, code-breakers resided in more modest living accommodations than today. Two examples were Dot Braden and Ruth "Crow" Weston. To make ends meet in Washington, they shared an apartment by bunking together while another roommate slept on the couch. When the women purchased a mattress, modern furniture delivery did not exist; so, the women bartered with the shopkeeper to drive the mattress to their apartment in return for preparing him scrambled eggs. Like many other workplaces at the time, code-breaking was no place for a "working mom." Although the Army was more tolerant of pregnancy, planned and unexpected, the Navy treated pregnancy as a disqualifying condition, whether joining or continuing service. Once Weston became pregnant, she wrote in her file, "I have to resign my position as a mathematician because I am needed at home with my baby." By telling these stories, Mundy shows implicitly how women's roles have evolved since World War II.

While the author, a veteran writer of women's issues, does glorify these women, she recognizes their challenges and the toll of the work upon them. As the US propaganda machine was steadily conveying a message of success to the public, the code breakers were privy to the grim realities of where the enemy was targeting, and whose husbands, fiancées or brothers were casualties of war. The secrecy of the mission was so isolating that even code-breaking roommates did not discuss their work with one another. As a result, many broke down, and some would abuse alcohol to cope with the stress and isolation. It was Post-Traumatic Stress Syndrome (PTSD) before it had a name or treatments. The US Government was slow to declassify these efforts, and families of the code-breakers would not learn until at least the 1990s that these women were doing more than some clerical function.

CONCLUSION

Liza Mundy succeeds in penetrating the prolonged OPSEC by bringing the story of women code-breakers to life. Not only *could* these 11,000 women do what was asked, they *did*, while also fighting an uphill battle of gender discrimination before the passage of civil rights laws that would mandate equal pay and decent working conditions. Mundy shows that the steadfast devotion to duty of these silent patriots contributed to the Allies' successes, and it is fitting that their stories are finally told, resulting in the admiration and recognition they richly deserve.

Title: *Code Girls: The Untold Story of the American Women Code Breakers of World War II*

Author: Liza Mundy

Publisher: Hachette Books
(October 2, 2018)

Paperback: 448 pages

Language: English

ISBN-13: 9780316352543

Price: $28

THE CYBER DEFENSE REVIEW

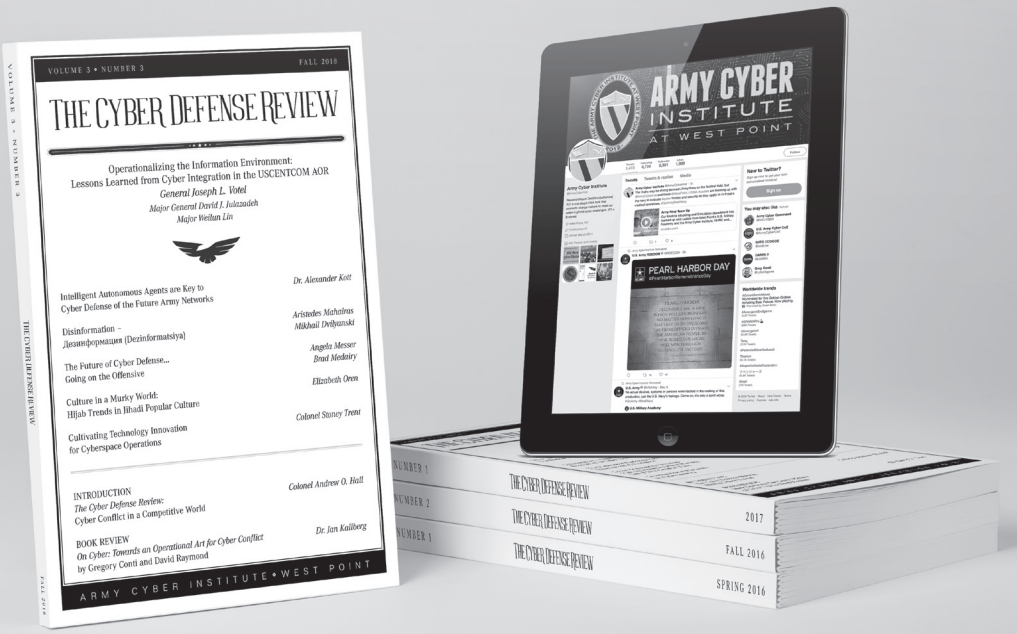
CONTINUE THE CONVERSATION ONLINE

cyberdefensereview.army.mil

AND THROUGH SOCIAL MEDIA

Facebook @armycyberinstitute

Twitter @ArmyCyberInst



ARMY CYBER INSTITUTE • WEST POINT

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.