VOLUME 2 ◆ NUMBER 2 SUMMER 2017

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT

The Cyber Defense Review

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

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

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

SUBSCRIBE
Digital: cyberdefensereview.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.
∞ Printed on Acid Free paper.

INTRODUCTION

SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

RESEARCH ARTICLES

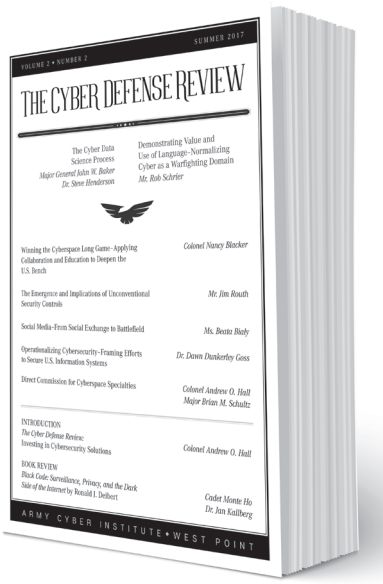
The Cyber Defense Review

Introduction

VOLUME 2 • NUMBER 2

The Cyber Defense Review: Investing in Cybersecurity Solutions

Colonel Andrew O. Hall



INTRODUCTION

We cannot truly predict how history will treat 2017, but with "WannaCry", "NotPetya" and election hacking, cyber conflict will be a major chapter. The latest ransomware attacks and their uncertain attribution continue to add complexity to an already wicked problem. The DARPA Cyber Grand Challenge created computers that could find and patch their own vulnerabilities, but we have much work to do incorporating artificial intelligence into a cybersecurity solution.

The future solutions lie in our multiple communities continued cooperative work to explore cyber conflict and the cyber domain. The International One Conference 2017 hosted by the Netherlands Ministry of Security and Justice and the Ministry of Economic Affairs highlighted the need for cooperation within as well as across governments. The NATO Cooperative Cyber Defence Centre of Excellence's annual conference, CyCon 2017 "Defending the Core", highlighted that balance of the vulnerabilities and opportunities of our digital world, as well as the asymmetries currently existing between our defense and offensive capabilities.

Our fourth edition of *The Cyber Defense Review* starts with two essays that address normalizing the Cyber Domain and increasing intergovernmental collaboration. The first essay comes to us from the Cyber National Mission Force Deputy Commander Robert Schrier, and the second from Colonel Nancy Blacker, currently stationed at the National Defense University. We round out our commentary section with an innovation piece by the Chief Security Officer of Aetna, Jim Routh.

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

The research section of this issue spans data science, social media, cyber situation awareness, and the defense of West Point. Dr. Dawn Dunkerley Goss shares insight from operationalizing cybersecurity at Army Materiel Command, and Major Brian Shultz and I explore direct commissioning opportunity for the U.S. Army.

This year, Palo Alto Networks' Cybersecurity Canon project added six new works to the list of books all cybersecurity practitioners should read. If you are not familiar with their project, I highly recommend reviewing Rick Howard's Cyber Talks March 2015 presentation which is available on the Army Cyber Institute's YouTube Channel. We finish this issue with a recommendation for and a review of the book by Robert J. Deibert's, "Black Code: Surveillance Privacy, and the Dark side of the Internet" by Cadet Monte Ho and Dr. Jan Kallberg. There is no shortage of new books on cyberspace and cybersecurity, and *The Cyber Defense Review* editorial team welcomes your submissions to review your favorites.

The Cyber Defense Review

Senior Leader Perspective

Demonstrating Value and Use of Language–Normalizing Cyber as a Warfighting Domain

Rob Schrier

ABSTRACT

Cyberspace has been recognized as a warfighting domain in the US Department of Defense (DoD), yet neither the DoD nor the broader US Government has taken full advantage of military cyber power to defend US interests and project power. One important reason for this is how we choose to consider and describe cyber. Do we treat it as no different from other domains and normalize cyber as a warfighting capability? Or do we recognize it as fundamentally different from other warfighting domains and use cyber-unique approaches? I believe the answer to both questions is "yes"—we need to further normalize cyber as a warfighting capability, yet recognize how it is different from the physical warfighting domains. The key to our future success lies in reconciling these two perspectives.

This essay lays out my perspective and offers recommendations, based on my experience with how we reached this fork in the road beginning in 2008 with Operation Buckshot Yankee. Since its inception in 2010, U.S. Cyber Command (USCYBERCOM) has made significant strides in helping operational commanders understand cyber capabilities and in how they need to be integrated into operational plans and maneuvers. The DoD, led by USCYBERCOM, has strived to normalize cyber into warfighting strategy, doctrine, plans and operations; but often these very actions make it difficult to recognize and optimize the unique capabilities that cyber can bring to a Combatant Commander, the Secretary of Defense, and the President. This article describes how we reached this fork in the road and how we can achieve a balance between the need to normalize cyber yet clearly articulate its uniqueness as a warfighting domain.

Mr. Rob Schrier is currently serving as the Deputy to the Commander, Cyber National Mission Force (CNMF), U.S. Cyber Command. He is a native of Silver Spring, Maryland who has over 35 years in federal service. He was a plank holder and part of the team who established U.S. Cyber Command and then served as the initial Deputy Director for Current Operations. Over the course of his career he has held a variety of leadership positions in the DoD after beginning his career as an analyst. Mr. Schrier has more than seven years' experience as a leader in cyber defense and cyber security. On his own initiative in the mid-1990s, he created the first successful operational Presidential National Performance Review Reinvention Laboratory within the U.S. Department of Defense, named *"Support to the Combat Operator."* Mr. Schrier has a Bachelor of Arts degree from the University of Maryland and a Masters of Science Degree in Applied Behavioral Science from Johns Hopkins University.

Stage Setters

A few recent illustrative snapshots helps set the stage. Recently USCYBERCOM Cyber National Mission Force leadership held a teleconference with a Director of Operations (J3) for a Combatant Commander (COCOM) on a major USCYBERCOM defensive cyber operation in his area of responsibility (AOR). At the end of the meeting, the J3 observed that we had conducted the entire meeting using fires and maneuver terminology with no "cyber jargon." He stated that we had made him comfortable as a J3 and enabled him to understand cyber as an element of his broader combat mission. So, in this instance, we were able to normalize cyber operations for the Combatant Command J3. He understood the Cyber National Mission Force operation, the risks involved, and how our operation supported his scheme of maneuver. In contrast, I recently attended a virtual meeting with a Combatant Commander and other senior DoD officials on a time-sensitive planning effort, and it was clear during the meeting that the normal doctrinal language USCYBERCOM used in explaining the cyber planning did not effectively convey the effects being proposed. In this instance, the appropriate doctrinal language was not effective in describing our cyber capabilities sufficiently for the principals to understand and apply them. To better understand the "normalization" challenge we need to briefly look back at 2008 and then at the evolution of USCYBERCOM.

Operation Buckshot Yankee, October 2008

In October 2008, the DoD discovered a serious, probably nation-state, infiltration of DoD classified military networks. While no one was certain how serious or significant this infiltration was, the DoD treated this intrusion as the potentially most dangerous type. The task of lessening the impact of this intrusion fell to Joint Task Force–Global

Network Operations (JTF-GNO), which issued a series of orders across the DoD to eliminate the use of thumb drives and to support additional DoD countermeasures. JTF-GNO issued their standard Communications Tasking Orders (CTOs), which are specialized orders traditionally reserved for the communications community and which apply solely to those channels. In this instance, the orders included significant, resource intensive actions that were counterintuitive to many communicators. JTF-GNO had issued specialized orders using very technical language without the proper operational context required for Commander's decision. Therefore, their approach was that of "IT administration" rather than operational necessity, and as a consequence, this critical effort was not consistently prioritized at the urgent level. Over the years, I have spoken with dozens of communications officers from all four Services, and they universally reported that the orders issued under Operation Buckshot Yankee made them feel frustrated and disempowered. In fact, several of the Communications Officers working during the operation in tactical locations admitted that they had trouble implementing the orders fully as the tasks simply did not make sense. Many Commanders simply had no context to appreciate the nature of the risk. The orders issued for Operation Buckshot Yankee were not immediately recognized as Commanders' business and a threat to national security systems was treated by many as Information Technology (IT). During this period, the Department was struggling with whether cyber should be treated as IT business or as a warfighting domain. Many senior DoD officials believe that Operation Buckshot Yankee was the catalyst for the Department standing up USCYBERCOM in May 2010.

USCYBERCOM—The Early Years

When USCYBERCOM stood up in May 2010, the primary mission focus was on Defending the DoD Information Network (DoDIN), and the secondary priority was full spectrum cyber support to the Combatant Commanders. USCYBERCOM spent the bulk of its energy and time creating the vision, strategy and doctrine for cyber as a warfighting domain and USCYBERCOM's role in that domain. There were numerous engagements on how command and control of cyber operations should evolve across the DoD and what role USCYBERCOM should have in DoDIN Defensive Cyber Operations given the responsibilities of the Services, Defense Information Systems Agency and the DoD Chief Information Officer.

Neither the DoD nor the broader US Government has taken full advantage of military cyber power to defend US interests and project power.

For the team creating and building USCYBERCOM Current Operations, we decided that a key to success was to demonstrate USCYBERCOM's value to the Warfighter and to cre-

ate trust across DoD and USCYBERCOM's ability to lead and synchronize Defensive Cyber Operations. We thought these keys were equally, if not more important, than creating vision, strategy, and doctrine. USCYBERCOM Current Operations leadership recognized the need for information and evidence gathered through practice and experimentation. We could not rely on a wholly conceptual framework. We set out to demonstrate the value of our newly launched Joint Operations Center (JOC) rather than straying into the debate over command and control with the Services, DISA, and the DoD CIO. Even if we made mistakes, we felt we had to start executing the mission and then assess, learn, and adjust. Through the JOC, we began to create a collaborative environment across the DoD by issuing orders that were designed to feel like operational maneuvers instead of IT administrative actions. The orders process itself was a lynchpin to our early success in the JOC. Soon after we stood up the JOC, we made what at the time was an unpopular decision to stop using Communications Tasking Orders and instead use the standard military orders process. We wanted commanders and their chiefs of operations to clearly understand the nature of our orders, to include the "why" and the "so what" in terms that would resonate with Commanders' overall operational functions. We also reinforced the process of pre-coordinating major orders, especially the more complex orders, to gain up front buy-in for those orders across the DoD. While this essay does not discuss any operational specifics during the first three years of USCYBERCOM, we were successful at starting to demonstrate value to commanders and building trust across the DoD. This took a great deal of time, effort and focus to achieve. The change in the orders process from communications orders to general orders, using English that clearly communicates and conveys the uniqueness of the cyber mission rather than forced formal doctrinal language, proved much more effective in helping Combatant Commanders understand this mission, the nature of the threat, and the intended effects that we could deliver.

We reached this fork in the road in how to achieve balance between the need to normalize cyber while clearly articulating its uniqueness as a warfighting domain.

Today (May 2017)

As a Department, we continue to focus energy and time on the DoD Cyber Strategy, establishing and improving foundational documents, studying cyber's value in deterrence, and describing cyber in classic military doctrinal language. Alternatively, the USCYBERCOM J3 continues to demonstrate value across the Department and to interagency partners on a daily basis. The USCYBERCOM Component Commands are all primarily

focused on demonstrating value by making progress against their assigned mission sets. I believe it is important to continue making that mission progress, demonstrating capability, and working to have those capabilities fully understood and embraced by the Combatant Commanders. In balance with our more strategic efforts, it is important that the strategy, policy, and doctrine communities keep listening to the operational community so that their thinking remains grounded in reality.

Normalizing Cyber as a Warfighting Domain?

So if we return to the question of whether we normalize cyber as a Warfighting domain or treat the domain as unique in certain ways, the answer must be both. We should move away from describing cyber solely in terms of existing military doctrine and strategy because cyber capabilities and missions do not fit neatly into existing doctrinal effects terminology or Phases 0 through 5 effects. We should recognize when these constructs do not fit cyber and use simple, clear language to communicate. We should also be precise in explaining how cyberspace is different from other domains, to include its man-made and dynamic nature, as well as the ways deeply cyber is deeply ingrained in every aspect of our lives.

We should move away from describing cyber solely in terms of existing military doctrine and strategy because cyber capabilities and missions do not fit neatly into existing doctrinal effects terminology.

My original assertion was that the US Government is not yet taking full advantage of employing cyber power to defend US interests and project power. I believe that describing cyber solely in terms of existing military doctrine and strategy is inhibiting us from fully utilizing our nation's military cyber capabilities. We need our Warfighting Commanders and the Interagency to understand exactly what cyber can and cannot do, and what the risks are in plain English. We need to keep demonstrating operational value, which will continue to build Commanders' confidence in the USCYBERCOM mission. Once we improve understanding and consistently demonstrate value, we will start to realize the opportunities which lie in cyber as a warfighting capability. The first step in doing that is to use plain English to describe cyber capabilities and effects.

Winning the Cyberspace Long Game – Applying Collaboration and Education to Deepen the U.S. Bench

Colonel Nancy Blacker

Since 9/11, collaboration, on any subject touching national security, has increased and improved among U.S. Government departments and agencies. While this improvement is welcome, it nonetheless waxes and wanes with various leaders. Though a bit of a generalization, it is a recognized truth that leaders with previous 'good experiences' throughout the interagency champion collaboration and those with 'bad experiences' stifle collaboration. Those with negative experiences are content to allow the 'small stuff' (time to meet, time to build personal relationships, time for education, and minor expenditures for travel) to present insurmountable obstacles to collaboration. In the quickly changing environment of cyberspace, this cannot stand. Blowing through bureaucracy is an imperative to the development of effective strategies and subsequent plans and actions that counter adversarial cyber operations. The Department of Defense (DoD), with a rather large share of the budget and doctrine that defines planning and execution, should take a stand across the inter-agency cultural divide and drive results-based collaboration. To apply a relatable metaphor, DoD needs to achieve results faster than it took Army to halt Navy's most recent football winning streak. National cybersecurity guidance mandates collaboration on many fronts, but does not speak to (nor should it) how to actually collaborate. Recent Congressional legislation guides and directs collaboration and reinforces this urgent need particularly in the cyber arena (e.g., Cyber Intelligence Sharing and Protection Act of 2016; Cybersecurity Enhancement Act of 2014; National Cybersecurity Protection Act of 2014; Federal Information Security Modernization Act of 2014, Cybersecurity National Action Plan of 2016, that supports and implements the Cyber Security Act of 2015).

COL Nancy Blacker is the Senior Military Faculty at the National Defense University's College of Information and Cyberspace. Previously, COL Blacker served as a Senior Military Advisor to the Assistant Secretary of Defense for Strategy, Plans, and Capabilities as Chief of Global Force Management for the Office of the Secretary of Defense for Policy. COL Blacker has served on the staff of two Combatant Commands (Pacific Command and Special Operations Command) focusing on counterterrorism and countering weapons of mass destruction. She has over 25 years of service in the US Army to include enlisted time before earning her commission through Officer Candidate School. COL Blacker deployed with the 25th Infantry Division to Iraq as the Economics Work Group Chief in the G3. She holds a B.A. in Geography/Urban-Regional Planning and a J.D. from the University of Kentucky.

The most recent U.S. Government direction to departments and agencies for cyberspace collaboration occurred on May 11, 2017, with the publication of President Trump's Executive Order (E.O.) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[1] In addition, President Obama's Presidential Policy Directive (PPD) 41, "U.S. Cyber Incident Coordination"[2] is also still in effect. Both of these documents constitute progress on the senior leader led front for interagency collaboration to strengthen national security, though PPD 41 refers to the narrow reponse based effort of coordinating "a cyber incident". President Trump's new cybersecurity E.O. focuses on managing cybersecurity risk and among other directives tasks agency heads to provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget within 90 days of the order.[3] President Trump also tasks the executive branch to submit strategic options to deter adversaries and better protect the American people from cyber threats.[4] This directive is a tall order and only amplifies the need to enhance the pathways to U.S. Government collaboration regarding the looming issues in cyberspace. While the cyberspace domain is becoming increasingly important as evidenced by the 2017 National Defense Authorization Act (NDAA) directing the elevation of U.S. Cyber Command (USCYBERCOM) from a sub-unified Command to a Combatant Command[5], cyberspace issues must nevertheless compete with other National Security priorities. While USCYBERCOM continues to mature its organizational structure to assume the mantel of Combatant Command (CCMD) authority and responsibility, it will need support and assistance to enable the collaborative ecosystem necessary to orchestrate global DoD cyberspace actions as a coordinating authority. There

are many ways to enhance collaboration, but two concrete approaches float to the top: (1) Designate the National Defense University's College of Information and Cyberspace as the primary institution to educate collaborative teams and build the bench for the future to address the requirements of emerging legislation and executive orders shaping US actions in cyberspace; (2) Increase cross pollination across departments and agencies through slight adjustments to personnel management practices (detailing, assigning, allocating, etc.).

National cybersecurity guidance mandates collaboration, but does not speak to (nor should it) how to actually collaborate.

USCYBERCOM's expanding authorities and competing global priorities are not the only challenges to working together in the cyberspace arena. Other turbulence to collaboration includes a lack of streamlined processes for both assignments and education across the US government, and an unwillingness to allow action officers the time to invest in building personal relationships across the various US departments and agencies. In a recent monograph by The Hon. Janine Davidson, Emerson Brooking, and LTC Ben Fernandes, they noted a cultural difference between military and civilian decision-makers at the senior level mainly defined by differences in age, education, and unique-to-the-profession experiences.[6] Taking these differences as a cost of doing the business of the Nation is an unnecessary toll. Why not remove some of the obstacles to collaboration through changes in assignment and personnel system mechanisms to allow different groups to get acquainted earlier in their respective careers instead of waiting until they meet at the National Security Council (NSC) level cloaked in distrust?

While greater collaboration yields positive results, in order to reap this advantage in cyberspace, the Nation needs to identify where cyberspace fits as a priority to identify risk and make the appropriate resourcing choices. By the sheer virtue of twenty-five years of increasing reliance on computers, not to mention other evolving technological advances, cyberspace concerns run through every national security issue. We communicate through cyberspace. Cyberspace enables us to talk confidentially—though many would argue and offer evidence to the contrary. Cyberspace enables and enhances command and control. Cyberspace enables and enhances capability. Cyberspace is ubiquitous in daily operations across the government and, therefore, cyberspace concerns should be funded in a manner corresponding to its current importance. The recent spate of legislation and Executive Orders emphasizing the importance of cyberspace must be complemented by appropriating the means to fund the execution of the guidance each contains and the results each directs. But the key to implementing the guidance and directives is an education path lighting the way for the action officer level to

gain critical understanding of the complex playing field of the cyberspace domain and, to provide a forum for such understanding to develop. Organizations along with their unique cultures should make modifications to not just support collaboration but to enable and encourage it. Currently, the cyberspace landscape seems disconnected. There are documents directing action (e.g., The Cybersecurity National Action Plan) and the establishment of organizations (e.g., the Cyber National Mission Force, U.S. Cyber Command, cyber organizations within various agencies) to implement the strategies and plans, but there are few formal opportunities and means to collaborate across the whole of government, particularly at the action officer level.

Obstacles to collaboration include a lack of streamlined processes for both assignments and education across the US government.

Previous Presidents have had cybersecurity chiefs or cyber advisors. President George W. Bush appointed Howard A. Schmidt as a cybersecurity advisor; President Obama appointed Mr. Schmidt as his Chief of Cybersecurity; President Trump has not named a separate cybersecurity advisor or chief outside of his current cabinet configuration. Mr. Schmidt oversaw several high-level exercises which involved participants from across the U.S. Government.[7] The exercises were an excellent idea and perhaps yielded excellent execution, but the problem remains that conducting such events at the highest levels only ensures that seniors are prepared for interagency events, it doesn't ensure or even encourage collaboration at the lower levels. Problem-solving power cannot rest only at the most senior levels of government. Teaching rising senior leaders how to navigate the cyberspace ecosystem will be the key to future solutions. There is no mechanism to coordinate the various cyberspace related documents, strategies, law, and plans at the federal level other than discussions at the NSC. Additionally, many Directors at the NSC do not have the requisite experience to address all the cyberspace related requirements emanating from the executive branch. This paper does not suggest an answer to that problem, but focuses on providing opportunities for various organizations to mesh together to generate the bottom-up ideas and actions that will ultimately deter, dispel, degrade, or attack our adversaries. The many aspects of the cyberspace domain, and the various ad hoc efforts to harness and understand the domain, make it imperative to identify opportunities to conquer cyberspace challenges. The greater community needs to make significant progress on collaborative efforts outside of discrete problem sets and reaction to a crisis. Short of creating additional bureaucracy at the federal level, it makes sense to provide a pathway that prepares action officer practitioners to execute meaningful whole of government collaboration. Such a pathway currently exists at the National Defense University College of Information and cyberspace. This pathway is narrow but could expand its capacity if directed and commensurately resourced.

Another way to make incremental process in the realm of collaboration in cyberspace, aside from educational opportunities at the College of Information and Cyberspace, involves tweaking personnel processes to routinize 'cross-pollination' throughout U.S. Government departments and agencies. This means that the barriers to placing DoD personnel in the Department of Homeland Security (DHS), or Department of State (DOS) personnel in DoD, or any other potential arrangement must be removed. This is much easier said than done because the barriers do not lend themselves to easy removal. Layers of bureaucracy, fortified by law and policy, confuse and limit moving personnel across agency boundaries. Certainly, personnel policies offer value and order. However, they should not present a permanent roadblock to collaboration. The situation cries out for innovative solutions. Clearly the Department of Defense is capable of innovation as evidenced by former Secretary of Defense Carter's establishment of the Defense Innovation Unit Experimental (DIUx) in 2016 (and its subsequent expansion after twelve months). This is a case of "more is better"—public-private ventures and other clever ways to harness the power of various department and agency personnel routinely working together will be the key to countering complex problems in cyberspace. The Nation needs not only to respond to cyber challenges but more importantly anticipate cyber requirements. Innovative and unique solutions (whether public-private or across the interagency) may, to paraphrase Emma Lazarus, "yearn to breathe free" and include out-of-the-ordinary personnel decisions.

The Nation needs to identify where cyberspace fits as a priority to identify risk and make the appropriate resourcing choices.

The Military Services are responsible per Title 10 U.S. Code to man, train, and equip the force [8] and therefore, have exclusive personnel policies and procedures. Similarly, other parts of the U.S. Code, as well as departmental policies, direct various agencies how to manage their respective personnel. Commonly, memorandum of understanding fill in the blanks where guidance does not exist on how to share or distribute expertise. When the opportunity arises to share or distribute expertise, each participating agency wins. Knowledge is gained and captured to spread around. Knowledge, if kept prisoner in its originating agency, will not contribute to the greater good. Any agency could lead an effort to make collaboration easier (sometimes documents name a lead federal agency (LFA)). But it makes sense, when a document is silent on the LFA, to designate DoD to lead interagency planning efforts, because of its proclivity for planning; i.e., concept plans and operational plans abound in the organization and are tools of collaboration with other agencies. Key cyber stakeholders can certainly come up with viable courses of action, but they will be doing so in a vacuum of peril, potentially reaching solutions that have not been vetted through the lower levels of interagency collaboration. Uninformed

solutions, ultimately briefed to principals or deputies at the NSC, present dangerous consequences. The best solutions will come from a collaborative effort at the action officer level across departments and agencies to share personnel and the skillsets that tackle complex cyberspace issues affecting national security. Again, the NSC level should not be one of the initial collaborative efforts. The looming risks of greater frequency and severity of cyberattacks against the US or its interests demand that action officers have a chance to pursue aggressive out-of-the-box solutions in the diverse interagency setting before bringing recommended solutions across the bow of senior decision-makers.

Teaching rising senior leaders how to navigate the cyberspace ecosystem will be the key to future solutions.

While untying the interagency Gordian knot looms large, we should not have to wait on King Henry V, through the keen observation from the Archbishop of Canterbury, to loosen it. "... Turn him to any cause of policy, The Gordian knot of it he will unloose" [9]. Increased opportunities for training and education across the interagency through formal channels should lead to strengthened relationships that facilitate planners and decision-makers at all levels of government. A focus on training and education should find its way through the jungles of personnel bureaucracy. But, to date, such a focus has not, and probably will not become an accepted practice, unless pushed or accepted or championed by senior leaders. The training and education can, and does, occur informally among agencies, but it would be infinitely better if it occurred as a routine option offered by an academic institution. One way to accomplish the goal of increased education and training opportunities is to house this effort in an established professional educational institution. The DoD possess a tremendous network of joint and service schools and centers of excellence. Thus, it makes sense for DoD to offer and sponsor interagency education with some of these opportunities existing at no cost to the recipient/student. As mentioned, DoD offers such an option for interagency participation with the College of Information and Cyberspace (CIC) at the National Defense University.

The CIC is currently set up to accommodate students from across US government departments and agencies, international governments, and the US private sector. The school has been operating since 1990 and offers approximately 40 graduate courses, multiple times per year, that can be combined into a variety of graduate certificate programs. The CIC also offers Joint Professional Military Education under the auspices of the Joint Staff, J7. The College is part of the National Defense University. Thus, with all this experience and administrative overhead already in place, the CIC is the perfect location for a new program at the strategic and operational level specifically designed to educate practitioners. Because the current curriculum is already varied and geared toward interagency education, it would be easy to expand the course offerings to specifically focus on

educating designated working groups focused on implementing directions in new (or relatively new) legislation and updated strategies.

The CIC designed its Chief Information Officer (CIO) curriculum in concert with key stakeholders, and it has worked well. The outcome of this curriculum clearly focuses on graduating students sliding into professional positions within the US government. For cyberspace, the departments and agencies need people who know cyberspace, know each other, and know how to work collaboratively. The CIC can accommodate this need easily because it has the infrastructure and the habitual interagency relationships already in place. What is missing is the formal tract for the interagency cyberspace professional. Education focused specifically on output to fulfill requirements in new laws, policies, and directives that can evolve by the same model as the CIC CIO certificate. But instead of focusing on the goal of turning out professionals to become CIOs, a new, more practical model could recognize and fulfill a need in the cyberspace realm to include joint and interagency collaboration to deliver recommended solutions that will more quickly and effectively make a difference in the cyber ecosystem. Solutions that could drive anticipatory action vice reaction.

Increased opportunities for training and education should lead to strengthened relationships that facilitate planners and decision-makers at all levels of government.

One of the biggest challenges to collaboration is literally a physical location to talk. Meeting space in the National Capital Region (NCR) is at a premium as are other challenges that seem like minutiae (parking, physical space, the right people, computer access, etc.) but ignoring these minutiae quickly adds up to absolute paralysis of action. Many practitioners can tell anecdotal stories about how some thing was not done because it was too hard to find a place to meet, gain support from leadership for time off, and get the right people to the table. NDU with its central location in the NCR overcomes all these obstacles and most importantly provides the appropriate academic environment to incubate innovative ideas to solving the most pressing cyberspace challenges.

Once prepared, new cyberspace leaders from across the interagency will be able to immediately make two separate but significant contributions to National Security: 1) lead, influence, or participate in any strategic or policy level cyber challenge at their respective agency; and 2) offer a rolodex of relationships to organize and reconvene at NDU to solve immediate pressing problems at the operational level. No other joint educational opportunity offers these outputs and options.

Conclusion—Keys to Success

SENIOR LEADER SUPPORT

It is imperative to have senior leader support at all levels for this action, particularly in DoD. Frequently, so many measures require senior leader attention that those items outside the Secretary of Defense's top five challenges (sometimes referred to colloquially as "4 + 1") get lost. The President has noted the importance of cyberspace, as have the CJCS and the Secretary of Defense. However, under budgetary constraints, it isn't that senior leaders don't recognize the importance of cyberspace, but rather they lack the resources (time, personnel, and/or money) to make collaboration work because they are otherwise occupied completing the required outputs within their own respective department or agency. Thus, the ecosystem is not nearly as connected as it could be.

Lacking fundamental resources, senior leaders are forced to prioritize operational priorities (both planning and executing) over in-depth interagency collaboration. However, NDU, as the Chairman's University, could easily provide a 'sandbox' for US government departments and agencies to not only receive pertinent strategic cyber education, but to actually conduct the collaborative actions necessary to turn out recommendations for senior leader approval for any designated LFA. It's as if all the best actors in the world are ready to put on a play (in this case, all the cyber subject matter experts from across the USG) yet they lack a place to rehearse and refine the dialogue to perform their masterpiece. That is what NDU can offer—the place to rehearse, the expert designers, editors, and teachers to provide guidance for the ultimate product—National Security.

RESOURCES TO PAY FOR THE ACTION

Priorities cannot be adhered to without the necessary resources. Sending rising leaders to a collaborative school, while low cost in the general scheme of maneuver, is nonetheless an expenditure. Whether the action costs time or money (or both), there will be a cost. Thus, back to the number one element (senior leader support)—without seniors recognizing a significant benefit to the risk of losing a productive staff member for some period of time, this proposition will never be implemented.

ASSESSMENT OF INITIAL OUTLAY OF EXPENDITURE

The Cost Benefit Analysis must be quickly established for this proposition to gain standing in the education pipeline. Therefore, the first class should be monitored by NDU and their contributory actions should be routinely reported through the Joint Staff to the Chairman of the Joint Chiefs of Staff and Secretary of Defense as well as through the respective leadership chains of the participating departments and agencies. An honest self-assessment can be accomplished.

KEEPER OF THE FLAME

NDU CIC as "keeper of the flame" would be responsible for assessments (to include a feedback and refinement loop), and for collaborating with key stakeholders to develop pertinent and appropriate curriculum. Once armed with assessment data, NDU will be able to put any residual costs in their base budget to support this effort. In addition, NDU CIC could designate a faculty chair to serve as home base for establishing a cyber strategy and policy rolodex to back up graduates of the program, serve as an information repository for departments and agencies, and to offer a backbone and model of future collaborative efforts.

NOTES

1. Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Federal Register 82, no. 93 (May 16,2017): 22391, https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.

2. Presidential Policy Directive 41, July 26, 2016, Directive on United States Cyber Incident Coordination, https://www.gpo.gov/fdsys/pkg/DCPD-201600495/pdf/DCPD-201600495.pdf.

3. Ibid., Executive Order 13800 of May 11, 2017.

4. Ibid., Executive Order 13800 of May 11, 2017.

5. National Defense Authorization Act of 2017 (NDAA 2017), Pub. L. No. 114-328, Section 923. [S.2943], http://congressional.proquest.com/congressional/docview/t41.d42.114_pl_328?accountid=12686.

6. Davidson, J.A., Fernandes, B.J., & Brooking, E. T. (2016). *Mending the broken dialogue: Military advice and presidential decision-making.* Council on Foreign Relations. Retrieved from http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1829719677?accountid=12686.

7. SCHMIDT, HOWARD. 2011. "Defending Cyberspace: The View from Washington." *Brown Journal Of World Affairs* 18, no. 1: 49-55. *Business Source Premier,* EBSCO*host* (accessed June 17, 2017).

8. Armed Forces, U.S. Code 10 (2011).

9. Henry V, Act 1, Scene 1, accessed from http://shakespeare.mit.edu/henryv/full.html.

The Cyber Defense Review

Professional Commentary

The Emergence and Implications of Unconventional Security Controls

Jim Routh

Cybersecurity control frameworks, the foundation of security practices in any enterprise today, are becoming less significant with the evolving cyber threat landscape–driving a response towards innovation in control design and resulting in the deployment of unconventional controls. Control frameworks will remain essential, but they alone are no longer sufficient to avoid significant data loss from cyber breaches. In some respects, this represents an 180° change from how our cybersecurity professionals were trained over the past several decades.

Cybersecurity curriculums within the military services and in the public education system have grown significantly in recent years due to the increasing demand for cybersecurity professionals in private industry and government agencies. This is a generally a positive development, although the shortage of cyber skills in the market makes it difficult for the enterprise to attract and retain cyber talent. Some professionals entered cybersecurity through opportunistic means by taking advantage of the significant growth in demand for practitioners in industry. More and more are entering the field today after seeking out cybersecurity curriculums in college or by serving in various military branches with advanced cyber training. All of us learned the importance of security control frameworks as a foundation for any public or private enterprise seeking to manage risk effectively.

Security control frameworks remain core foundational components of cybersecurity programs, and I don't believe this will or should change. But I can't help acknowledging that when I first learned cyber security risk management techniques and practices, they were directly aligned with control standards from authoritative sources that represented the most maturity for enterprise adoption. The majority of the enterprise control standards for private industry in the past several decades were derived from

Jim Routh, CISM, CSSLP, CSO is the Chief Security Officer and leads the Global Security function for Aetna. He is the Chairman of the NH-ISAC Board. He serves on the Board of the National Cyber Security Alliance and is a member of the Advisory Board of the ClearSky Security Fund. Mr. Routh was formerly the Global Head of Application and Mobile Security for JP Morgan Chase. Prior to that he was the CISO for KPMG, DTCC and American Express.

Jim is the winner of the 2016 Security Alliance Award for Innovation, 2016 ISE Luminary Leadership Award, the Northeast and the 2014 North American Information Security Executive of the Year for Healthcare, the 2009 BITS Leadership Award sponsored by the financial industry in collaboration with NIST and the Department of Treasury.

authoritative sources (e.g. NIST 800-53, ISO-27001, FISMA, COBIT, and COSA). The maturity of the enterprise's security program was directly tied to the results of testing controls to determine if the enterprise practices were aligned with the control standards linked to authoritative sources, depending on the applied regulatory framework. Control standards (often referred to as policies) are documented and periodically tested by auditors or security assessors. The more stable the results from the testing of controls, the more mature the program. So as cyber professionals, we learned that changing business models, system architectures—and even the hiring and firing of people—all led to changes with direct implications for practices that evolve outside the alignment with controls and, therefore, opportunities for remediation and further testing.

The more consistent the business was with steady growth, the easier to prove cyber security maturity through alignment to the framework and consistently positive control testing results. Actual certifications (often conducted by third parties) resulting in the attestation of effective controls assures senior management and stakeholders about the resiliency of the security program. The underlying assumption was that the more change in control implementation, the less mature the program. In other words, if control standards changed continually, it was the result of an immature program that was "fixing" or remediating the practices to align with the control framework. In some cases, senior cybersecurity leaders that moved from one organization to another often increased the number of changes to control standards and practices as a direct result of the transformation of the program under their leadership. Once the new controls and practices were implemented, the program maturity took hold

(alignment of practices to control standards), and recertification or another assessment confirmed the improvement in resiliency. Ingrained in my thinking was that the number of changes to control standards was directly correlated to the maturity of the overall security program; more changes to controls meant less resiliency, while few changes meant maturity and higher program resiliency.

What I've learned recently is the opposite of what I learned decades ago: the number of changes to control standards today is actually an indicator of maturity, not immaturity. Unlike in the past, consistently changing control standards today is actually an indicator of resiliency in a program. Consistent changes to control standards or procedures indicate an active response to changes made by threat actor tactics, resulting in higher resiliency and greater maturity for a cybersecurity program. The fundamental difference is that the cyber threat landscape is changing more rapidly than any other time in our history (a trend likely to continue). In fact, the introduction of IoT in the marketplace is further accelerating the growth of the attack surface, and the growth in capturing consumer behavioral data is leading to a faster evolution of the cyber threat landscape. Essentially, when threat actors adjust their tactics (professional criminal and nation-state sponsored threat actors), it is most often due to either advances in controls by enterprises or new attack surfaces available from consumer product innovation. Cyber threat actors seek the most efficient way to achieve their objectives with the least amount of effort. If enterprises respond by consistently changing their controls, they can create friction for threat actors who adjust their tactics. Ensuring that an enterprise is a less attractive target is about as good as it gets for a CISO and is dependent on the nimbleness of adjusting controls.

Control frameworks will remain essential, but they alone are no longer sufficient to avoid significant data loss from cyber breaches.

This subtle shift, which changes the orientation of a CISO, does not mean control frameworks and testing controls are no longer valid means of measuring resiliency or program maturity. It simply means that testing controls against a framework is one data point representing a snapshot in time. It is an indicator of maturity and resiliency at a point in time. Another indicator of resiliency is how often control standards and procedures change in response to changes to the threats. The road to cyber program maturity will likely include the adoption of a set of control standards and a control framework. Aligning the framework with an authoritative source (or many) remains a part of the critical path to program maturity and remains an important component of a cybersecurity program. Security leaders need to recognize that the conventional controls defined within a framework alone will likely be inadequate to manage risk in a sustainable way. This is

not because the frameworks are no longer effective. The reality is that the threat landscape is more diverse and changes more rapidly for any framework to keep up with. Most meaningful changes to policy frameworks come about over time, as consensus among subject matter experts influence the need to update the standards. Risk frameworks with annual changes and updates are about as frequent as is practical. This pace of change, although admirable given the difficult work of codifying changes, is misaligned with the evolution of the threat landscape. As security practitioners, we have to evolve our practices driven by the changes in threat actor tactics. Keeping up with the changes to risk frameworks alone is insufficient, assuming we wish to keep our leadership roles.

Security control frameworks remain core foundational components of cybersecurity programs, and I don't believe this will or should change.

I went through a cycle over four years ago where I transformed a cybersecurity program from one based on regulatory compliance to one driven by risk and, specifically, changes to the threat landscape. I measured the number of control standard changes or adjustments made. In the early days of the transformation, control standards and procedures changed all the time. Daily changes were common. Over the three-year period, I assumed (incorrectly, it turns out) that the pace of changes introduced to control standards, procedures and practices would decrease dramatically. Today, the program is approaching its fifth year, and the average number of policy changes is one per day. We are converging the cyber and physical security programs which will result in more policy changes. When we change a control standard or, more frequently, a control procedure, it is triggered by a change in practices aligned with the new control requirement. Almost every control standard has several key performance indicators that measure the health of the process where the control is imbedded, and that is monitored frequently. One of the KPIs that carries more weight is how many changes are introduced (control standards, procedures, and the corresponding practices), and the average is one per day.

I've learned that a risk-driven security program needs to change security posture measured through the control standards and procedures at the same pace as threat actors who adjust tactics. This year, daily changes may be the right indicator of both maturity and resiliency, but next year it may be one and a half changes daily; the next year, two changes. It will never again be once a month or once a quarter or annually. I still remember the drudgery of changing the security policy document once a year and how I never thought there were significant changes made when I began my career in security. Today, significant changes happen every day in the policy, practices and measures of enterprise residual risk. We measure our enterprise risk trend daily and share it with

senior executives to help them understand what influences changes to risk. One of the most interesting aspects of this daily pace of change is that the majority of the changes in controls are in a category we call unconventional.

Conventional controls are well established within risk frameworks and clearly defined. In addition, the audit testing procedures are mature, well established, taught to others and repetitive. When external auditors test for identity and access management controls today, the methods and techniques used for sampling and testing control effectiveness are based on decades of practical experience and are well documented. Auditor skill level is measured and quantified through certifications and ongoing education (see ISACA.org) for industry, including The American Institute for Certified Public Accountants (AICPA) certifications. Auditor opinions matter, but the methodologies used are mature and established as effective.

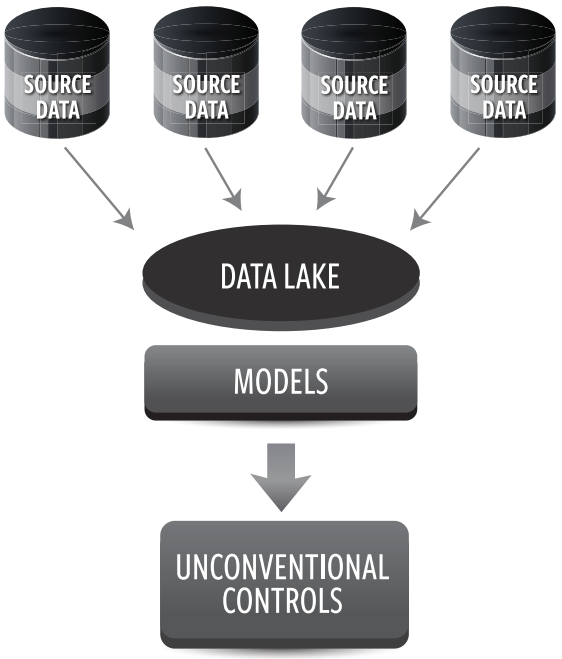
What I've learned recently is the opposite of what I learned decades ago: the number of changes to control standards today is actually an indicator of maturity, not immaturity.

Unconventional controls are not easily identified within the most commonly used risk frameworks and represent innovation, either in the technology capability being applied or in the techniques applied by the security practitioner. Unconventional controls often result in either a new control standard or, at a minimum, new control procedures. Here is an example of an unconventional control standard and its implications.

Conventional controls for monitoring and controlling access for privileged users (those with the entitlement rights to add or delete accounts like domain or server administrators) are well established in all control frameworks, as are auditing practices related to monitoring privilege users. We do not use conventional controls for privilege user management, a more important control objective given the fact that all cyber incidents involving data exfiltration required some kind of breach or bypass of privilege user rights. This puts more of a premium on controlling for the misuse of privilege user rights or credentials being used by a threat actor to exfiltrate sensitive data. Instead, we use behavioral risk models to create patterns of use for every person or account with privilege access for a temporary period of time. The user patterns are derived from four sources of data:

1. Entitlement data
2. Web browsing data from the web proxy
3. Email usage data from the data loss prevention log data
4. Physical access data

These patterns or models are used in real time to identify anomalies or behavioral events that don't match a pattern. The pattern matching creates a risk score for the privileged user based on all of the attributes collected and analyzed in real time. We define specific risk score thresholds established for the types of privileges provisioned so when an anomalistic event or series of events breaks a behavioral pattern; the risk threshold determines one of two required actions. If the behavior score is within a specific range of tolerance, an email is automatically generated to the privilege user's leader asking them to confirm that anomalistic event is reasonable or not. If the leader response to the email is no (big red button), then the security operations center is notified to begin intrusive monitoring. If the behavioral risk score is high and above the threshold, then the specific entitlements are revoked for the privileged user automatically with no human intervention. The security operations center is notified as is the leader of the privileged user. Essentially the effectiveness of the primary control is tied to the behavioral risk model. The more data on the behavior of the user, the better performing the model is.



One of the first questions I typically receive when describing this model for privilege user management is about the accuracy of the models. The answer is that for over four thousand users with privilege for a specific period of time, we typically get a handful of anomalies a day and a large majority of the alerts received are benign or modifications that go back into the models.

One of the biggest implications for the implementation of this type of unconventional control is not in the implementation effort itself (which was relatively easy to do) but in the auditing of the effectiveness of this unconventional control. This privilege user management (PAM) control represents a growing trend of applying models to real-time access management, a trend that is accelerating as security practitioners build and implement better machine learning capabilities. This trend makes the job of the auditor more complicated and challenging, requiring the testing of models to determine their control effectiveness. Unfortunately, there is no body of data or techniques for testing models established over the decades of control testing in practice. The use of an unconventional control, like this one for PAM, requires new testing procedures and techniques for the auditors.

I'll provide another example of an unconventional control that has significant implications for both security architectures and auditing procedures. In this case, this unconventional control has implications for any IT or security professional designing applications now and in the future, and the trigger event is directly related to changes made by threat actors to bypass access controls for web and mobile applications. Threat actors today have access to billions of credentials (user ids and password combinations) harvested from security breaches and posted to public sites along with Social Security Numbers (SSNs) available in Dark Web forums. The result is that binary authentication, a one-time event at the front end of a user interaction with a web or mobile application, is becoming obsolete. Passwords (including one-time generated passwords) are becoming less effective as an access control since this control is based on the difficulty of the threat actor getting access to the factor or factors. The number of successful login events today in any large enterprise that is actually someone with credentials from a legitimate user is increasing due to the availability of the credential and SSN information to criminals. The net effect is an evolving obsolescence of passwords as a primary user access control, and that has significant implications for how we design application architectures going forward.

> Ensuring that an enterprise is a less attractive target is about as good as it gets for a CISO and is dependent on the nimbleness of adjusting controls.

A number of security professionals are now moving beyond passwords to deploy behavioral models using many attributes of online behavior and to create a pattern for each user across mobile and web channels. The behavioral attributes are collected during account registration and refined with more online account usage, creating a risk score to which the application can react in real-time so the actual authentication event is integrated into the user lifecycle of the application, rather than occurring one time at the beginning of the

lifecycle. The sensitivity of the application allows the application to respond to the behavioral authentication risk score and provide the level of access commensurate with the risk score at any point in the user's experience with the application. The number of architectural constructs that change in this kind of behavioral authentication is significant for the security professional, the application designer, the developer and the auditor.

This is another case of the use of an unconventional control in response to changes in threat actor tactics that has significant implications for determining the effectiveness of the control—and conventional risk frameworks do not offer much in the way of guidance for the auditor. Security professionals need to evolve control standards and procedures in response to shifts in threat actor tactics, which means enterprises must change how they build and deploy technology architecture and create more challenges for the auditors dealing with model-driven controls in real-time that are clearly key controls (heavily relied on for risk management). Sometimes the enabling technology available from an early-stage company offers game-changing capability for the enterprise. We are implementing an authentication model using behavioral risk scoring from patterns that also enables us to make adjustments to authentication controls without changing application code, saving millions of dollars every year. Changing authentication controls quickly provides the enterprise with more resiliency to respond to changes in threat actor tactics, avoids the need for developers to write or change application code every time we make an adjustment to an authentication control, and saves on operating costs. This is another positive outcome for pursuing unconventional controls.

A few years ago, I hired a chief data scientist, formerly with the National Security Agency, exclusively for the security program. His contribution to raising the skill level in data analytics for security professionals has been instrumental in our ability to deploy unconventional controls in response to changes in the threat landscape. What I had no idea of at the time was that his deep skills in data science would be so important to helping auditors figure out how to test unconventional and model-drive controls throughout the enterprise going forward.

Security professionals who understand that risk-driven programs are essential to improving resiliency for the enterprise are reaching beyond conventional control frameworks and creating unconventional controls enabled by models. These unconventional controls have the potential for mimicking another highly resilient system called the human immune system. Antibodies responding to threats automatically are essential to the human immune system and models driving unconventional controls are becoming more essential to the enterprise.

The Cyber Defense Review

Research Articles

The Cyber Data Science Process

Major General John W. Baker
Dr. Steve Henderson

Our world is facing explosive growth in data being communicated on and generated by its people, their systems, and their networks. More data has been created in the past two years than in the entire previous history of mankind (Heidorn, 2016). By 2020, our digital universe of data will grow to 44 zettabytes (or 44 trillion gigabytes) which is ten times its size today. The enormity of this data and our ability to apply advanced technology to leverage it to gain new insights is often described as the era of "big data." The study and application of big data spawned a new interdisciplinary field known as data science which combines the domains of operations, mathematics, and computer science as well as several ancillary fields such as social science, intelligence, and economics. The application of data science has already shown great promise in a wide range of fields from medicine to business.

Because of these achievements, there is a natural expectation that the U.S. Army will equally benefit from data science, particularly in the data-rich area of cyber security. Based on data science successes in the civilian sector, the Army hopes to leverage its data to increase cyber situational awareness, maintain clairvoyance about its networks, and achieve information dominance over its adversaries. As we described in our previous article (Baker & Henderson, 2016), data produced on and by military networks defines the very contours of military cyber operations and must be mastered by the Army to gain a competitive advantage against our adversaries. In the words of Google's Eric Schmidt, "the Pentagon needs its own Google for all its data" (Defense One, 2017). In the spirit of helping the Army leverage its data at Google-like levels, we presented the case for a cadre of Army data scientists to lead this effort. Our recommendation follows the analysis of the problem and reflects trends and best practices observed in

Major General Baker is a 1985 graduate of Norwich University and was commissioned a Lieutenant in Armor. He served his initial assignment with the 1st Squadron, 3rd Armored Cavalry Regiment. He was branch transferred to the Signal Corps as a Captain.

MG Baker has commanded signal units at every echelon; company, battalion, brigade, theater, and now NETCOM, a global command.

He holds Master's Degrees from Central Michigan University and the Industrial College of the Armed Forces. He is a graduate of the Armor Officer Basic and Signal Officer Advanced Courses, Command and General Staff College, and Industrial College of the Armed Forces.

Major General Baker and his wife Laurie have two daughters, Alexis and Mackenzie.

government and non-government entities adapting to a data-fueled revolution that is impacting everything from cybersecurity to logistics to health care (The White House, 2014; Verizon RISK Team, 2015).

As the Army moves quickly to seize on opportunities presented by data, there is a natural tendency to focus on 'the what and who' aspects of a solution. What technology do we need to design, purchase, and engineer? Who do we recruit, train, and develop to use this technology? Who leads this effort? However, much less attention has been devoted to how these personnel and technologies are specifically brought to bear on cyber operations. In this paper, we outline the *Cyber Data Science Process* to addresses this question. The Cyber Data Science Process is a workflow of specific activities that define how data science should be incorporated with cyber operations. It combines the latest in data science research with doctrine and best practices found in military intelligence and targeting activities. We include a functional analysis of the workflow and identify the actions, skillsets, and products required at each stage.

Our national security requires the U.S. Department of Defense (DoD) and other agencies having guaranteed access to a reliable, secure, and accessible network at all times. This network is known as the Department of Defense Information Network (DODIN). Data science and its associated processes are key requirements to the network's security and resilience. The Army Network Enterprise Technology Command (NETCOM) provides the Army's portion of the DODIN, ensuring freedom of action in cyberspace while denying the same to adversaries. A major implied task in NETCOM's mission is gaining and maintaining complete situational awareness about what is happening on its networks. However, there are a number of challenges that make this task difficult.

Dr. Steve Henderson is a Senior Cyber Security Research Scientist working in the Software Engineering Institute at Carnegie Mellon University. He is an accomplished computer scientist and systems engineer with over 23 years of experience in the Department of Defense community defining requirements, designing solutions, implementing systems, and leading teams to solve complex technical challenges. Steve is also a retired U.S. Army Lieutenant Colonel. He holds a Ph.D. in Computer Science from Columbia University, an M.S. in Systems Engineering from the University of Arizona, and a B.S. in Computer Science from the United States Military Academy.

The first challenge is related to the evolving implementation of DoD cyberspace doctrine. Cyber operations are defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (JP 3-12). Within the DoD, cyber operations fall under the purview of the U.S. Cyber Command (USCYBERCOM) and its component commands: Army Cyber Command (ARCYBER), Fleet Cyber Command, Air Forces Cyber (AFCYBER), and Marine Corps Forces Cyberspace Command (MARFORCYBER). The capable men and women of these commands are trained and equipped to handle a broad range of offensive and defensive cyber operations and work with a number of non-military agencies to secure our national interests in cyberspace. In support of ARCYBER, NETCOM personnel operate the DODIN and participate in defensive cyber operations (DCO) conducted on their wide-reaching enterprise. This exceptional team of soldiers and civil servants do a tremendous job of keeping our network safe, healthy, and online. Nevertheless, they are not staffed, trained, or equipped to handle cyber operations informed by data science at levels equivalent to their potential adversaries. And, we must assume these same adversaries will use data science techniques to get past our strategic defenses to compromise our lower level networks. If we want to maintain complete situational awareness and freedom of maneuver on these networks, it is imperative that we staff, train, and equip NETCOM personnel to conduct data science informed DODIN and DCO operations at a sufficient level of capability.

A second challenge facing the Army deals with analyzing data generated on its networks. These networks span 20 countries around the globe in support of Unified Land Operations, 32 major commands, over 800,000 people, and operating 1.1

million devices. Collectively, these users and their machines generate 20 terabytes of data daily. In order to maintain situational awareness, five Regional Cyber Centers (RCCs) monitor portions of this data for events such as network intrusions, service interruptions, and suspicious network flows. However, RCCs are not resourced to completely leverage all the data at their disposal. What is needed is an ability to conduct state-of-the-art, large-volume, near real-time data science akin to best practices employed by our partners in industry (Marr, Bernard, 2016; Russom, 2011). These analytics could enhance Indications & Warning (I&W) capabilities and bolster incident response and real-time targeting data shared with USCYBERCOM. The analytics could also help inform orders generation, identify and forecast advanced threat behaviors, tune sensors, prioritize systems administration activities, and guide engineering efforts. Fully leveraging all the data generated on our networks is essential to out-maneuvering our adversaries in cyberspace and ensuring freedom of maneuver.

While we clearly need to address these cyber operation and data science man, train, and equip challenges we identified a third, equally critical, challenge. We submit that the Army needs to develop and validate a process to guide how we integrate data science capabilities into cyber operations. Even if Army units have sufficient people, experience, training, and tools to conduct cyber operations complemented by data science, how would these capabilities be best employed? What is needed is a detailed doctrinal process that governs how powerful data science capabilities can complement and augment our current military staff and decision-making practices. This process should be based on industry best practices, support current military doctrine, and provide sufficient detail to guide how we task-organize and operate to fully leverage data science in cyber operations.

The application of data science has already shown great promise in a wide range of fields from medicine to business.

ANALYZING INTELLIGENCE & TARGETING PROCESSES

Toward this end, we looked for inspiration from two types of processes found in military science: intelligence collection & targeting. Based on our experience, we believe these two analogs offer great insight for applying data science to cyber operations. Both intelligence gathering and targeting place the enemy at the center of our analysis and complement terrain-based approaches that focus on technical infrastructure. The added emphasis on the enemy helps augment traditional security models focused on incident handling and compliance (Security for Business Innovation Council, 2012). This is especially important in cyber operations where the enemy is comprised of hundreds of attackers daily ranging from non-nation to nation-state actors, to organized criminals, to hactivists,

to novice script kiddies. Most of these entities operate in isolation and are pursuing different, uncoordinated objectives while employing different tactics, techniques, and procedures (TTPs). Thinking about cyber defense as a one-size-fits-all model treats these threats equally and fails to address nuances that are exploited by the attacks. Instead, we need an intelligence-focused approach that focuses our defensive posture and can be applied across a wide array of bad actors simultaneously, targeting and out-maneuvering each with synchronized and well-coordinated cyber operations.

We examined several well-known processes from the intelligence and targeting realms. Our goal is not to replace these processes because each plays an important and established role in military operations. These processes provide support to military decision making and can be directly applied to cyber operations. Rather, our goal is to analyze the processes to determine how they can inform a more detailed and low-level process to help the Army data scientist.

The first process we examined is defined in DoD Joint Publication 2.0 (JP 2-0, 2013) which describes a general doctrinal intelligence process practiced within the DoD. This process, shown in Figure 1, is followed by each component service, though some services may choose to augment certain steps.

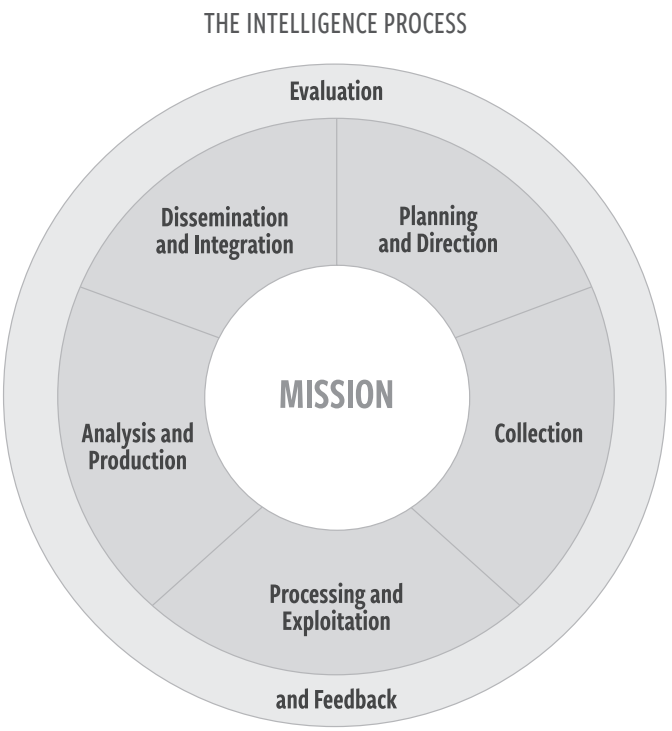


Figure 1. The JP 2.0 Intelligence Process

The DoD joint intelligence process involves five sequential phases that are centered on supporting a particular mission and reinforced by continuous evaluation and feedback. The first phase, Planning and Direction, consist of outlining the specific intelligence activities and actions required to support the mission. This includes prioritizing and directing intelligence collection efforts and assets. The collection phase of the process involves the physical act of acquiring intelligence data and information from human, imagery, signal and other intelligence sources. The Processing and Exploitation Phase involves activities to collate, clean, store, and organize collected intelligence information for follow-on exploitation and analysis. The exploitation portion of this stage involves an initial and rapid review of processed information to identify high-value and time-sensitive information that can immediately support the mission. The Analysis & Production stage is a deliberate activity to carefully study, review, and combine the various intelligence information and produce one or more intelligence products. These products include, but are not limited to, reports, estimates, briefings, and diagrams. The final stage, Dissemination and Integration, involves distributing various intelligence products to units and individuals and integrating analysis and recommendations into current and future operations.

We submit that the Army needs to develop and validate a process to guide how we integrate data science capabilities into cyber operations.

As a potential candidate to guide data science, the Joint Intelligence Process presents several strengths and weaknesses. One strength of the model is that each of its component stages are data-driven activities that provide natural opportunities to apply data science. For example, the process and exploitation stage involves analytical tasks that are performed with data science techniques including pattern-recognition, natural language processing, and machine learning. A second strength is shown in how the continuous evaluation and feedback activity encourages a work flow where data analytics are reviewed and improved throughout the entire process. On the negative side, the process is fairly high-level and doesn't specify many details on how specific data science functions should be performed in each step. Moreover, the intelligence process isn't necessarily presented with a view toward cyber operations. Finally, the main phases of the intelligence process are sequential with no intermediate opportunities to iterate or go back to a previous step.

The next process we examined in detail is a cyber-focused intelligence process known as the Cyber Intelligence Lifecycle and developed by the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force, Tactical Cyber Intel (INSA, 2015). The process, which is shown in Figure 2, has seven steps.

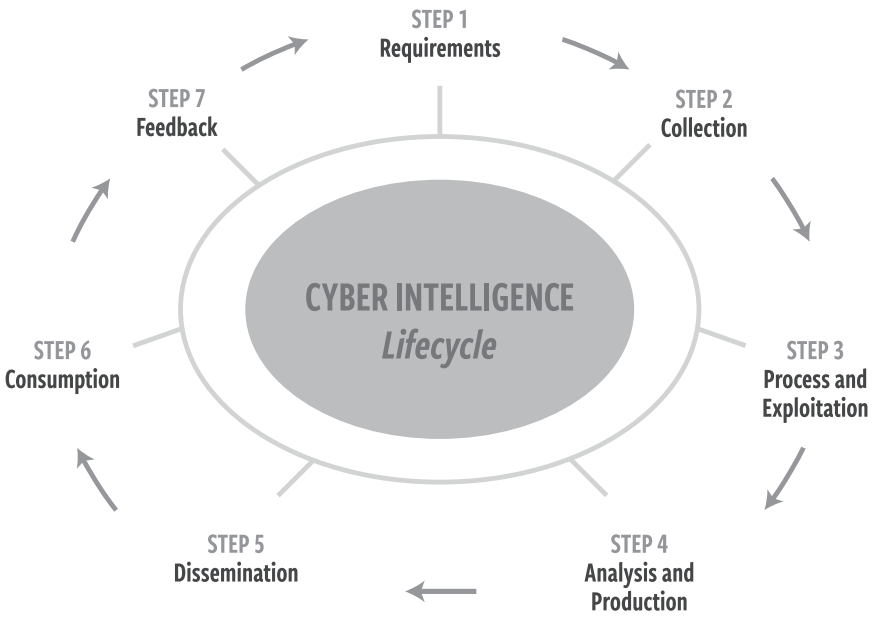


Figure 2. Cyber Intelligence Lifecycle

Step 1 defines the requirements for the overall intelligence process. This involves enumerating what intelligence products and outcomes are needed to support the mission. Requirements flow from analyzing the current environment, organizational goals, essential aspects of the mission, and previous threat intelligence. This includes deriving a detailed network map and enumerating possible data sources. Step 2–5 cover collection, processing, exploitation, analysis, production, and dissemination and are similar to related functions in the JP 2.0 joint intelligence cycle. Step 6 entails an explicit consumption function, which involves ensuring intelligence outcomes and products are integrated with the decision-making process and acted upon in a timely and sufficient manner. Step 7 entails reviewing these generated and consumed intelligence outcomes to determine if the original requirements were satisfied.

The strengths of this model are its enumeration of requirements and consumption activities as dedicated steps in the lifecycle. The requirements elicitation step ensures the process defines specific outcomes to satisfy stakeholder and mission needs. This helps keep the intelligence process agile, mission-focused, and relevant. The deliberate consumption step makes it the intelligence analyst's responsibility to ensure products they develop are consumed by the stakeholder. This encourages a continuous dialog between the analyst and the stakeholder to ensure requirements are met. The model shares the same weaknesses as the Joint Intelligence model; mainly it lacks specificity for data science tasks and it not internally iterative.

We next examined the Find, Fix, Finish, Exploit, Analysis, and Disseminate targeting process or F3EAD (U.S. Army, 2010; Faint & Harris, 2012). This process, depicted in Figure 3, is a tactical-level process developed to help Army units identify, target, and exploit high-value individuals (HVIs) across an enemy organization.

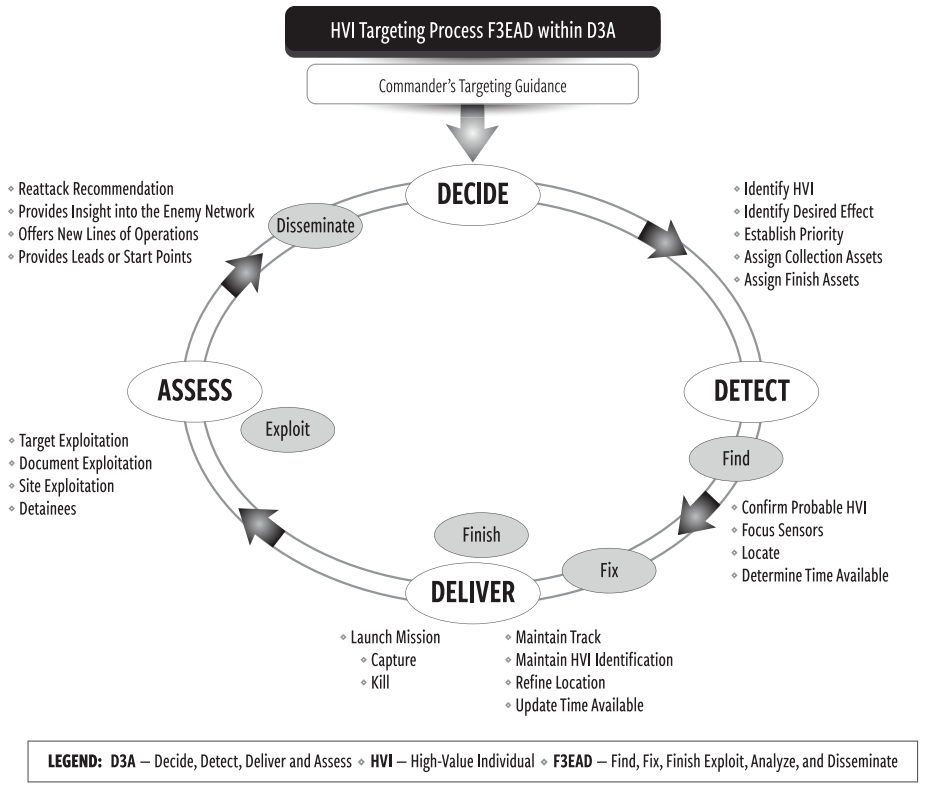


Figure 3 : F3EAD Targeting Process (U.S. Army, 2010)

The process has four high-level functions. The Decide function is the process of establishing a prioritized list of potential targets, what effect is desired for each (i.e. captured, killed, neutralized), and what intelligence and operational assets (i.e. drone, special operations, host-nation law enforcement) to apportion to each target. Detect is the process of finding and fixing each target using allocated intelligence assets. The Deliver function is launching operational assets to deliver the desired effect on each target. The delivery is followed by the deliberate exploitation of each target which includes prisoner interrogation, reviewing captured documents, and harvesting data from digital evidence. The Assess function involves analyzing this exploited information to determine new intelligence that is disseminated to inform additional operations. This includes adding new targets to the prioritized targeting list heading into the next iteration of the F3EAD process.

The strength of this model is its focus on specific enemy targets. The prioritized targeting process drives deliberate resource allocation for intelligence and operational assets. As part of a data science model, this same focus would provide explicit direction to the data science team about which analytics should be written to locate which targets. This would provide clarity and specificity to the team's efforts. However, a prioritized targeting approach would face limitations in the cyber domain. Not every threat to our networks represents a clearly identifiable entity we can track. Zero day vulnerabilities, unintended and unknown functionality caused by imperfections in the software design process, leave our systems vulnerable to the first threat actor that can identify the zero day and exploit it. While certain classes of threats would be traceable to High Value Individuals, the sheer size of our networks and the anonymity and obscurity offered by cyberspace technology make the targeting process highly dynamic and abstract. Data science can help illuminate this abstraction and may lead to refinement of how we think about targeting in cyberspace. For example, high-value targeting could be expanded to include High-Value Behavior, High-Value Organization, and High-Value Network Infrastructure. The highly iterative and agile nature of the F3EAD model can serve as an excellent framework for thinking about data-science supported targeting in cyberspace.

As a potential candidate for integration with the intelligence and targeting models, the Data Science Workflow presents several strengths and weaknesses.

DATA SCIENCE PROCESSES

Because we are interested in the application of data science to cyber operations, we also examined data-centric processes. Relevant work traces back before the emergence of data science to the age of the database. In this era, large, single-instance, industrial-strength databases powered academic research and business operations. Great interest was placed on extracting novel information from these databases which led to the fields of Knowledge Discovery in Databases, or KDD (Klösgen, 1996; Klösgen & Zytkow, 2002), and Knowledge Discovery and Data Mining, or KDDM (Reinartz, 2002; Cios, Swiniarski, Pedrycz, & Kurgan, 2007). These fields are collectively referred to as knowledge discovery process (KDP) for which Kurgan and Musilik provide an excellent survey (2006). Notable work includes an ad-hoc model outlined by Brachman and colleagues (Brachman, Khabaza, Kloesgen, Piatetsky-Shapiro, & Simoudis, 1996) which was extended to a foundational KDD model by Fayyad, Piatetsky-Shapiro, and Smyth (1996). This model defines a seven-step sequential process consisting of identifying goals, creating target data sets, data

preprocessing, data transformation, data mining, pattern evaluation, and knowledge presentation. The model places particular emphasis on the data mining step which is the process of applying algorithms to find patterns in data. Another important model, known as Cross Industry Standard Process for Data Mining (CRISP-DM), was created by an industry consortia consisting of International Business Machines Statistical Package for the Social Sciences (IBM SPSS), National Cash Register Corporation (NCR), Daimler Chrysler, and the Dutch banking company Onderlinge ziektekostenverzekeringsfonds van Hoogere RijksAmbtenaren (OHRA) (Shearer, 2000). The CRISP-DM model consists of six steps: business understanding, data understanding, data preparation, modeling, evaluation, and deployment. It still enjoys broad acceptance in the business world.

While the KDD and CRISP-DM models provide excellent foundations for creating a knowledge management process in any organization, they are abstract models that deliberately leave specific implementation details open to interpretation. Several researchers proposed additional models to add this specificity. These include work by van der Heijden who proposed the Process Mining Project Methodology (2012). This model includes specific data science tasks such as tool selection, data preparation, and decision model validation. Sipoloa applies the Fayyad's KDD model (Fayyad et al., 1996) to identify anomalies in network traffic (Sipola, 2015). In doing so, he adds specific data mining functions such as feature extraction, normalization, dimensionality reduction, and classification to the process (Juvonen & Sipola, 2012). Guo conducted extensive research into research programming, or the process of using computer programs to obtain insights from data

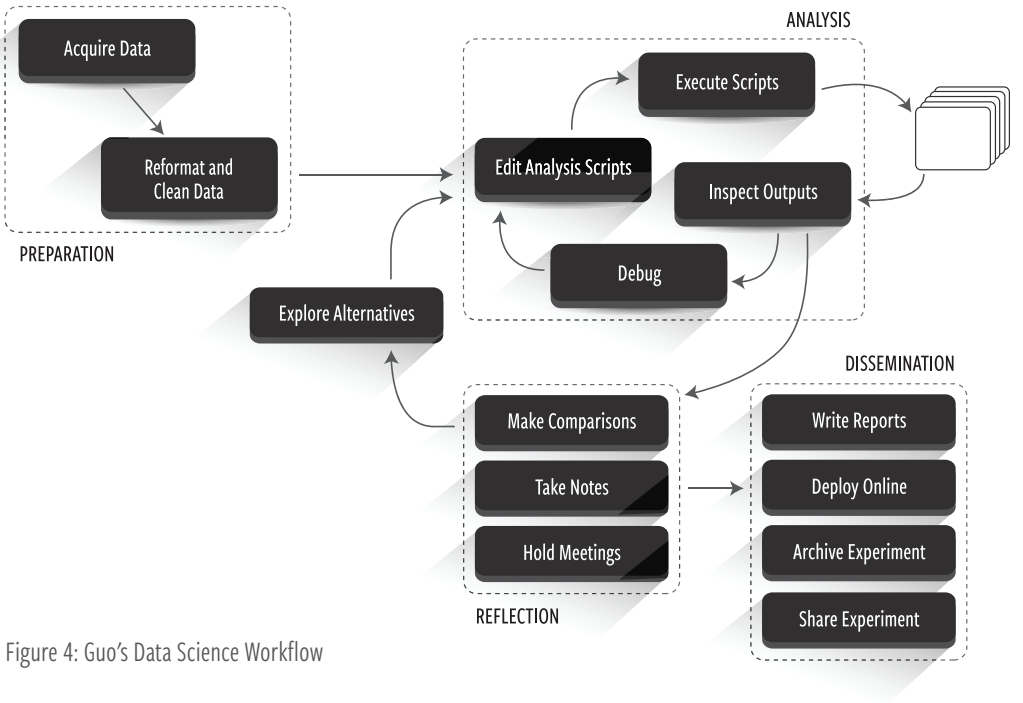


Figure 4: Guo's Data Science Workflow

(Guo, 2012). As part of this work, he proposed the Data Science Workflow consisting of four major phases (preparation, analysis, reflection, and dissemination) which each include detailed data science tasks.

Of this prior work, we selected Guo's model for further analysis because it captures the main phases found in the CRISP-DM and major KDD models while including additional detail specifically focused on data science. Within overarching stages of Preparation, Analysis, Reflection and Dissemination, Guo introduces several specific tasks. These are depicted in Figure 4.

The exploitation function involves an initial and rapid review of newly processed information to identify high-value and time-sensitive information that can immediately support the mission.

The preparation stage first involves acquiring the data, and then reformatting and cleaning it for follow-on analysis. From there, the process enters an analysis loop where the data scientist edits analysis scripts (computer programs) that are used to process the data. When these scripts are executed, they produce multiple outputs that can include statistics, tables, metrics, and charts. These outputs should provide new insights into the data scientist's questions. The data scientist inspects these outputs and, if not conclusive, debugs them, and then edits and runs them again. Once the outputs are verified, the data scientist carefully reviews them in the reflection phase. Outputs are compared against each other for accuracy and trends, and the data scientist invites others to collaborate on the findings. Documentation is critical in this phase, and the data scientist makes detailed notes about observations, limitations, and decisions made regarding the output. If required, further analytical product alternatives are explored to help confirm findings, address gaps, and eliminate inconsistencies. This spawns another cycle of the analysis loop. Once the data scientist arrives at a set of verified and validated outputs that provide new information they are finally ready for the final phase: dissemination. In this phase, the scripts used to produce the candidate outputs are put into regular production where they can augment existing business processes and workflows. The data scientist also takes time to write a formal report that archives and shares the experiment.

As a potential candidate for integration with the intelligence and targeting models, the Data Science Workflow presents several strengths and weaknesses. Two strengths of the model are its iterative nature and its enumeration of specific data science tasks that are performed at each stage of the model (e.g. writing scripts, producing charts, inspecting outputs). The main weakness in the model is that it assumes the model's research

questions and other information requirements are previously defined. The model does not include process steps for eliciting or defining what data should be collected or what questions deployed analytics should answer. A common retort to this criticism is that the system will just collect everything and be agile enough to answer any question within the organization's purview. While this may be true, it does nothing to inform the data science team's direction.

ANALYSIS

Our efforts to formally combine the data science, intelligence, and operation processes begin with a functional analysis of the intelligence and targeting processes to identify opportunities to apply data science to cyber operations. The goal of this analysis is to discover the overarching functions that occur in the operations and intelligence processes that drive military cyber operations. Once these functions are identified, we can begin to address how they might be supported by data science. The first stage of this analysis, depicted in Figure 5, is a functional grouping of the common functions found in the intelligence and targeting processes. We identified the functions in each process (the individual cells in Figure 5) and used an affinity diagramming process (Parnell, Driscoll, & Henderson, 2008) to group like-sounding functions into clusters. We then derived a cluster title (the table header in Figure 5) based on the predominate activity that occurs in each cluster (columns in Figure 5). The resultant clusters represent a core set of functions that occur in intelligence and targeting operations. These functions are summarized below.

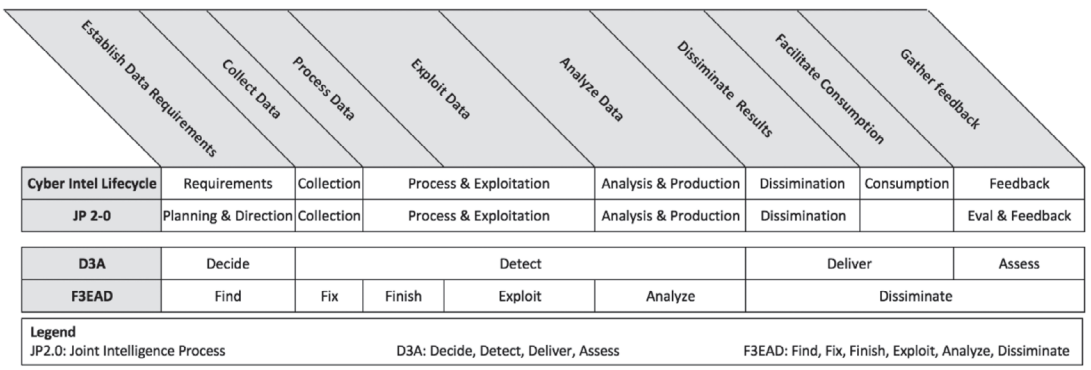


Figure 5: Functional Analysis of Intelligence and Targeting Processes

Establish Data Requirements. The Establish Data Requirements function is concerned with explicitly specifying what data is needed to inform the rest of the intelligence and targeting process. We believe the notion of requirements, which is enumerated in the Cyber Intel Lifecycle, is a critical function that encapsulates the planning, directing, and decision activities defined in the other intelligence and targeting processes. Requirements represent the outcomes we hope to achieve in cyber operations, and are driven by our

national security strategy, our related campaign plans, and the vision of our leaders. These requirements will vary at different echelons. Moreover, they are not fixed, need modification to adapt to changes in our operational and network security environment, and the actions of our adversaries.

Example data requirements include:

- Identify compromised systems within a certain network enclave
- Detect abnormal behavioral patterns by external entities communicating with DODIN assets

Collect Data. The Collect Data function is the act of sensing, storing, and transporting data collected on our networks. This can range from a brute-force approach where everything is collected to a more targeted set of data. The data science team should collect as much data as possible that addresses the requirements without compromising their ability to complete the other steps in the process in a reasonable amount of time.

Process Data. The Process Data function is focused on normalizing, cleaning, and pre-processing the data for follow-on exploitation and analysis. Automated techniques to help translate, classify, and tag the data with machine learning algorithms can markedly aid in this step.

Exploit Data. The Exploit Data function is the act of reviewing the data for analysis opportunities. Analysis can be an expensive and time-consuming process. Therefore, an initial review of the data needs to occur to prioritize where we conduct deeper analysis.

Analyze Data. The Analyze Data function is the application of qualitative and quantitative methods to transform the data into a meaningful result. A meaningful result is defined as one that supports one or more requirements defined in the Establish Data Requirements function.

Disseminate Results. The Disseminate Results function is concerned with communicating the results of data analysis with the decision maker, staff officers, other analysts, and curators of the data requirements. This process is quick and continuous in nature. An "always-on" approach aided by artificial intelligent agents that promote and vocalize results can greatly aid in this step.

Facilitate Consumption. The Facilitate Consumption function is a deliberate effort to ensure the disseminated results are consumed to help address data requirements. Of note, only the Cyber Intel Lifecycle included this function. One could argue that this function is not explicitly enumerated in other processes because it is a subtask of dissemination. However, upon further reflection, we believe treating consumption as a distinct function from dissemination is warranted. A data-driven intelligence and targeting process conducted around cyberspace will involve zettabytes of data. As such, there is the potential for a deluge of analytical products, reports, charts, and dashboards that could be

produced with this data. Therefore, there needs to be a deliberate and dedicated function to ensure the right analytics get consumed by the right people to make the best decisions. The data science team must devote time coordinating with other analysts, staff officers, and decision makers to understand their workflows and from where they derive their information. The data science team should then tailor and format analytical results to integrate directly with these workflows. This coordination should be done face-to-face.

Gather Feedback. The Gather Feedback function is concerned with working with the decision-maker and other stakeholders to ensure the consumed results of our analysis are actually satisfying our data requirements. This includes verifying and validating both the results and the process used to generate those results. Just because we have a product that reports a certain result, can we trust it?

We next turn to combining the intelligence and targeting processes with Guo's data science process. One approach we considered was simply applying Guo's entire process as a sub-function of each of our eight functions shown at the top of Figure 5. For example, Guo's entire process could naturally nest within the Analyze Data function. Even the Gather Feedback function could benefit from an embedded data science process to help gather and analyze usage data and user behavior. However, we concluded this is a simplistic treatment of data science that will preclude it from reaching its full potential in cyber operations. Data science is much more than a tool or technique to increase the ease and efficiency of our current process. Rather, it is an entirely new approach to how we synthesize, produce, and consume intelligence and operational information in the era of big data. Therefore, we need a more holistic examination of how data science can be integrated with our intelligence and operations processes.

Therefore, we juxtaposed Guo's top level functions–preparation, analysis, reflection, and dissemination–alongside our 8 functional clusters. The results are shown in Figure 6.

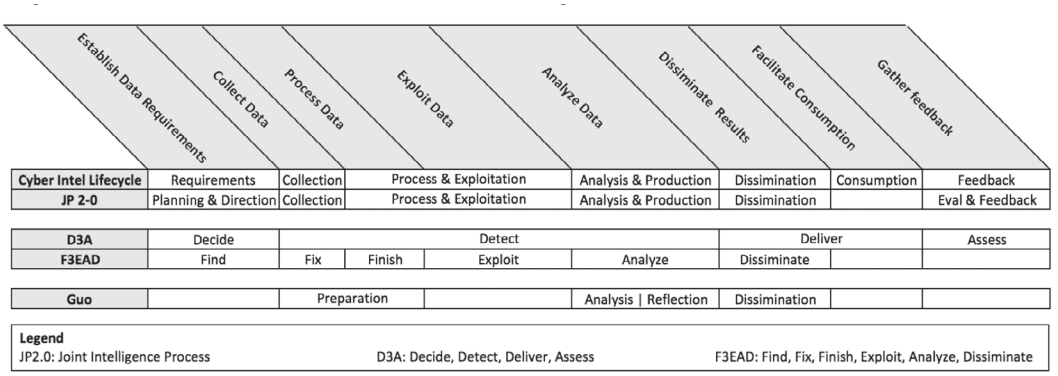


Figure 6: Functional Analysis of Intelligence, Targeting, and Data Science (Guo) Processes

This revealed several interesting findings. First, much of Guo's process lines up well with our military intelligence and targeting processes. However, as previously noted, Guo's process has no upstream requirements. We also noticed that Guo's process has no explicit notion of exploitation. It can be argued that exploitation occurs in reflection, but this happens well after analysis so would involve a significant delay. We believe a data science process should feature an opportunity for early exploitation before significant time is invested in analysis. Next, we noticed feedback in Guo's model is confined to the analysis loop and immediately following the reflection phase. But no feedback occurs outside the process to refine what data gets collected. Finally, Guo's model does not address consumption.

CYBER DATA SCIENCE PROCESS (CDSP)

There needs to be a deliberate and dedicated function to ensure the right analytics get consumed by the right people to make the best decisions.

Based on this analysis, we produced a hybrid process we call the Cyber Data Science Process, which is shown in Figure 7. This process model combines the functions from the intelligence and targeting models with Guo's data science process, building on common functions and addressing gaps. It is extremely important to note that this process is theoretical, and is intended to serve as a conceptual framework for thinking about how to best integrate data science into cyber operations. In practice, the entire CDSP process has to occur within the decision cycle of decision makers; else the entire effort lacks benefit from a military standpoint. Therefore, a data science team may choose to abbreviate, augment, or skip entire portions of the CDSP to accomplish the mission. Our aim is to provide concepts, functions, and terminology to inform the data science team's development of its internal practices.

The CDSP has seven functions, and merges the four major data science functions from Guo, with the functions identified in our functional analysis of the intelligence and targeting process. Each of the CDSP functions are described in detail below.

Establish Requirements. The goal of this function is to establish what data science outputs are needed to ensure friendly force mission accomplishment in the presence of cyber threats and the overall network environment. We emphasize that, at this stage in the process, the focus remains on data science outputs, and not on data science inputs (i.e. what data is required for collection). This is challenging, as it's difficult to envision products and outputs that will result from hours of prototyping, iteration, and testing. However, focusing on what product is needed—a resource decision, identification of a specific target, detection of an enemy operation—will ensure requirements are correctly

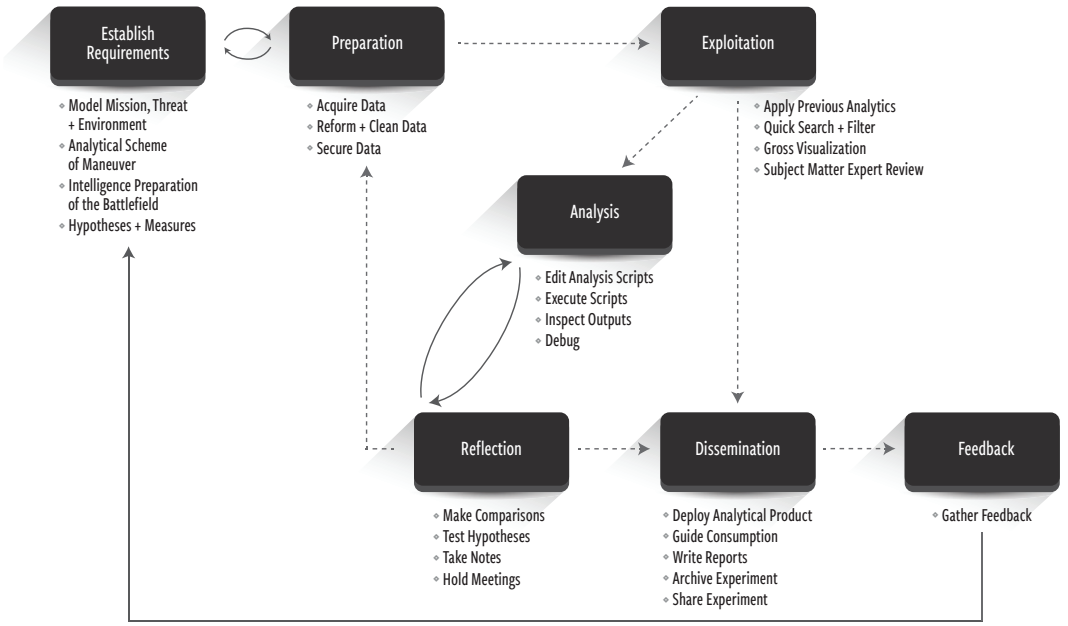


Figure 7. Cyber Data Science Process

established. We propose the data science team first develop models of the friendly force mission, the threat, and the environment. These shape what Parnell and colleagues define as the current state (the "what is") and the desired end state (the "to be") (Parnell et al., 2008). Modeling the mission, threat, and environment produces graphical diagrams, simulations, and mathematical models. This effort might include intelligence preparation of the battlefield process (IPB), an established modeling process integral to lethal military operations (U.S. Army, 1998). Recent work offers a cyber perspective (Winterfeld, Steven P., 2001; Harrison Kieffer, 2016) on the IPB process. Modeling should also include enumerating assumptions, limitations, and constraints relative to the friendly force mission, the enemy, and the environment. The data science team should then specify an "Analytical Scheme of Maneuver" (Stanton, Paul, 2017) to think through the analytical questions, how they relate to one another, how they support the mission, and when and what analytical outputs are needed. The data science team can then form hypotheses that help measure the progress of moving from the current state to the end state. For example, a current state of affairs might involve a suspected threat operating on our networks. The desired end state is the elimination of this threat from the networks. A corresponding hypothesis for this example might entail confirming, or failing to confirm with certainty, the presence of certain network signatures. Once hypotheses are identified, the data science team can draft measures, or metrics, that later confirm or

fail to confirm, the hypotheses. These measures directly define what data is required in the next phases of the CDSP. The ultimate product from this phase is a set of formally documented hypotheses and associated data science requirements. Skills required in this phase include data science, cyber operations/intelligence expertise, network systems engineering, mathematical modeling, human behavior modeling, and simulation engineering.

Preparation. The goal of the preparation function is to identify, collect, and transform all data needed to address the requirements. The hypotheses and associated metrics defined in the requirements function drive what data must be acquired, how much data is needed, and how often it is updated. Preparation includes determining where data collection sensors are placed in the physical word and cyberspace, which entities they monitor, and how data is routed from sensors to persistent storage. Once collected, the data is transformed for follow-on analysis. This is a significant task involving capturing data from sensors and moving and consolidating this data to a persistent data store. A typical cyber security environment can include a wide variety of sensors that collectively produce an extremely high volume of data at high velocities. These range from systems capturing raw network packets traveling at 1000 bits per second to others capturing the hundreds of minute changes that occur on each computer system. These sensors are typically not collocated in the same geographical location, so sensor data is moved to a separate persistent data store where it is available for follow-on analysis. From there, the data is secured to prevent the enemy from manipulating the data to deceive our analytics. The data is then reformatted and cleaned. Reformatting includes actions to store the data in a format that is compatible with the persistent data store. These actions might first include decrypting, decompressing, unpacking, renaming or filtering the original sensor data. Then, data is parsed, translated, and mapped from its native schema into the schema of the persistent data store. The data is then cleaned. Data cleaning, also known as data normalization, is the process of ensuring data integrity and involves deliberate steps to address incomplete, duplicate, or inconsistent records. The ultimate product of this phase is an accessible and persistent data repository containing all the data needed to explore the hypotheses; and, free of error. If this cannot be achieved, the data science team may need to return to the Establish Requirements function. For example, the team may discover they lack sufficient storage or computation resources to prepare the data originally scoped in the Establish Requirements function. Through additional analysis, the team may realize they can accomplish the same requirements with an extract of the

The Cyber Data Science Process is theoretical in nature, and must be adapted to match the speed and tempo of specific missions and their associated decision cycles.

original dataset. Skills required for the Preparation function include data science, data architecture, database administration, computer science, information technology administration, and network systems engineering.

Exploitation. The exploitation function involves an initial and rapid review of newly processed information to identify high-value and time-sensitive information that can immediately support the mission. The products of this stage are results from currently deployed analytics, charts, and scripts that immediately answer current or past hypotheses. New scripts or analytical products are not required, and the data science team must resist the urge to launch a new analysis expedition. Instead, the data science team refreshes previously constructed queries and analytics to identify any changes to the status quo or spot obvious items of interest. For example, a simple query searching through network traffic for a discrete set of target IP addresses might return a hit on newly ingested data. The data science team should fully leverage automated systems in this stage to programmatically select, execute, and summarize previously designed scripts and queries. The exploitation phase should also include some level of gross visualization which we define as automated charts and maps that track aggregate trends in the data. Consulting subject matter experts (SMEs) from the cyber mission and intelligence domains is critical in this stage. Their experience and intuition can identify trends and opportunities in the data and refine requirements for follow-on analysis. If the Exploitation function answers the mission-focused data requirements, the data science team can proceed directly to the Disseminate function to share these results. Skills required for the Exploitation function include data science, information visualization, and cyber operations/intelligence expertise.

Analysis. The analysis function of the CDSP involves authoring and editing scripts to test the hypotheses created in the Establish Requirements stage. This function includes an internally iterative process similar to the Analysis phase of Guo's workflow (Guo, 2012). This may involve writing multiple candidate scripts that each attempt to address the hypotheses in different ways. The data science team initially runs and tests these scripts on a subset of data loaded on local computing resources (i.e. a local cluster, server, or workstation). Once tested on an extract of the data, the data science team uploads the scripts into a production data science computing environment such as the Army and Defense Information Systems Agency (DISA) Big Data Platform (Bart, 2016). These environments feature a cluster of scalable computing resources with distributed computing technology such as Apache Hadoop or Spark. These clusters can efficiently apply the newly coded scripts against extremely large amounts of data at Petabyte scale. Even though the new scripts are running on the production environment, they should be designated with a development status until approved for dissemination. Once the scripts are complete, the data science team can inspect their output. This involves

examining raw output files and creating visualizations for output data. From these results, the data science team must verify the scripts' output matches intended behavior. If not, the data science team must redesign and debug the script. The ultimate product of this phase is a set of verified analytics (script outputs) that potentially answer hypotheses from the Establish Requirements phase. Skills required in this phase include data science, computer science, mathematics, statistics, machine learning, and information visualization.

Reflection. Once the data science team has a set of validated analytics, they enter the Reflection phase. The goal of this phase is to determine if the hypotheses from the Establish Requirements phases are answered by the analytics. The team makes comparisons and selects which analytics answer the hypotheses in the shortest amount of time with the least probability of error. Documentation and collaboration is essential in this phase, and the data science team should engage the decision maker, SMEs, and other stakeholders to solicit feedback from the newly scripted analytics. If the analytics do not meet the requirements, then the data science team may need to return to the analysis phase and redesign scripts. Or, the team may determine that more data, or data from additional sources is required to answer the hypotheses and return to the Preparation Phase. The ultimate product of this phase is a set of analytics that allows a decision maker to answer the hypotheses. Skills required in this phase include data science, computer science, mathematics, statistics, machine learning, information visualization, and cyber operations and intelligence expertise.

We believe the CDSP process, which integrates core functions from intelligence, targeting, and data science contains the necessary steps in sufficient detail to guide data science teams as they are integrated into Army cyber operations.

Dissemination. The end products for this phase are permanently deployed analytics running in the production data science environment that are regularly consumed as part of broader cyber operations workflows. In the short term, this involves making the new analytics, previously tagged as developmental, fully accessible to all relevant stakeholders on the production system. The analytics are integrated into dashboards and similar tools and fully documented. The analytics are carefully secured to ensure the enemy does not compromise our data-driven decision-making processes. Additionally, the data science team works to educate and train cyber operators and other stakeholders to adopt and consume the new analytics as part of their regular workflows. In the long

term, the data science team should report their efforts to the broader community and archive any results. Skills required during this phases include data science, data architecture, information technology administration, and training.

Feedback. The final phase of the CDSP is feedback. The outcome of this process is a regular review of the deployed analytics' performance, validity, relevancy, and data sources. Performance data—latency, accuracy and resource consumption—is compiled and reported for each analytic. Likewise, each analytics' data sources are reviewed to ensure their integrity. For example, collection may suddenly be interrupted for a data source supplying an analytic which could drastically alter its output. Any issues can prompt a redesign of an analytic. The data science team should also collect and review usage data about how users consume the analytic. A change in consumption could equate to a training deficiency, a loss of confidence in an analytic, or changing information requirements. The original hypotheses are reviewed to ensure they are still relevant to the organization's mission and operations. If these have changed, the entire process is restarted to address evolving requirements. Skills required during this phases include data science, data architecture, and information technology administration. The team should fully leverage automation in this phase to make the consolidation and reporting as easy as possible.

CONCLUSION

In this paper, we outlined the Cyber Data Science Process (CDSP) as a means to guide the application of data science to cyber operations. We believe this process, which integrates core functions from intelligence, targeting, and data science contains the necessary steps in sufficient detail to guide data science teams as they are integrated into Army cyber operations. It is important to remember that this process is theoretical in nature, and must be adapted to match the speed and tempo of specific missions and their associated decision cycles. We also feel this process is implementation and technology agnostic and can be successfully applied at various echelons and across teams of varying size and composition. Moreover, by answering the "how will data science be applied" question, the CDSP helps frame the next set of important questions—who will perform data science in the Army and what capabilities will they need? Toward this end, the CDSP helps specify what skillsets are needed, at what levels, for each of its functions. The process also helps scope task organization options and defines how many soldiers and civilians are needed to keep it running at a particular echelon. It also provides insights into the types of tools and technologies needed in each of its steps. Successfully addressing all of the questions will ensure the Army is well-positioned to realize the promises of data science, increase cyber situational awareness while maintaining information dominance over our adversaries.

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

Baker, J. W., & Henderson, S. J. (2016). Making the Case for Army Data Scientists. *Army,* 66(8), 41–43.

Bart, Daniel V. (2016). Big Data Platform (BDP) and Cyber Situational Awareness Analytic Capabilities (CSAAC). Presented at the AFCEA Defensive Cyber Operations Symposium. Retrieved from http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/4-Bart_Big-Data_Platform_Cyber.pdf.

Brachman, R. J., Khabaza, T., Kloesgen, W., Piatetsky-Shapiro, G., & Simoudis, E. (1996). Mining business databases. *Communications of the ACM,* 39(11), 42–48.

Cios, K. J., Swiniarski, R. W., Pedrycz, W., & Kurgan, L. A. (2007). The knowledge discovery process. In *Data Mining* (9–24). Springer. Retrieved from http://link.springer.com/content/pdf/10.1007/978-0-387-36795-8_2.pdf.

Defense One. (2017, January 9). The Pentagon Needs Its Own Google For All Its Data, Says Eric Schmidt - Defense One from http://www.defenseone.com/technology/2017/01/pentagon-needs-its-own-google-all-its-data-says-eric-schmidt/134456/(accessed January 26, 2017).

Faint, C., & Harris, M. (2012). F3EAD: Ops/Intel Fusion "Feeds" The SOF Targeting Process. *Small Wars Journal,* 31(7), 54pm.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine,* 17(3), 37.

Guo, P. J. (2012). *Software tools to facilitate research programming.* Stanford University. Retrieved from http://pgbovine.net/publications/Philip-Guo_PhD-dissertation_software-tools-for-research-programming.pdf.

Harrison Kieffer. (2016). Can Intelligence Preparation of the Battlefield/Battlespace Be Used to Attribute a Cyber-Attack to an Actor? *Cyber Defense Review,* (Spring 2016).

Heidorn, B. (2016, November). *Data Science Panel Discussion.* Sierra Vista, AZ.

INSA. (2015). *Tactical Cyber Intelligence.* Intelligence and National Security Alliance. Retrieved from https://issuu.com/insalliance/docs/insa_tacticalcyber/1.

JP 2-0. (2013). *Joint Intelligence.* Department of Defense.

Juvonen, A., & Sipola, T. (2012). Adaptive framework for network traffic classification using dimensionality reduction and clustering. In 2012 *IV International Congress on Ultra Modern Telecommunications and Control Systems* (274–279). https://doi.org/10.1109/ICUMT.2012.6459678.

Klösgen, W. (1996). Knowledge discovery in databases and data mining. In *International Symposium on Methodologies for Intelligent Systems* (623–632). Springer. Retrieved from http://link.springer.com/chapter/10.1007/3-540-61286-6_186.

Klösgen, W., & Zytkow, J. M. (2002). Knowledge discovery in databases: the purpose, necessity, and challenges. In *Handbook of data mining and knowledge discovery* (1–9). Oxford University Press, Inc. Retrieved from http://dl.acm.org/citation.cfm?id=778216.

Kurgan, L. A., & Musilek, P. (2006). A survey of Knowledge Discovery and Data Mining process models. *The Knowledge Engineering Review,* 21(01), 1–24.

Marr, Bernard. (2016, September 9). Big Data In Banking: How Citibank Delivers Real Business Benefits With Its Data-First Approach. *Forbes.* Retrieved from http://www.forbes.com/sites/bernardmarr/2016/09/09/big-data-in-banking-how-citibank-delivers-real-business-benefits-with-their-data-first-approach/#4bed2d1775ed.

Parnell, G. S., Driscoll, P. J., & Henderson, D. L. (2008). *Decision making in systems engineering and management.* Wiley-Interscience.

Reinartz, T. (2002). Handbook of Data Mining and Knowledge Discovery. In W. Klösgen & J. M. Zytkow (Eds.) (185–192). New York, NY, USA: Oxford University Press, Inc. Retrieved from http://dl.acm.org/citation.cfm?id=778212.778241.

Russom, P. (2011). Big data analytics. *TDWI Best Practices Report, Fourth Quarter,* 1–35.

Security for Business Innovation Council. (2012). *Getting Ahead of Advanced Threats.* RSA. Retrieved from https://www.rsa.com/en-us/resources/achieving-intelligence-driven-information-security-synopsis.

Shearer, C. (2000). The CRISP-DM model: the new blueprint for data mining. *Journal of Data Warehousing,* 5(4), 13–22.

Sipola, T. (2015). Knowledge Discovery from Network Logs. In *Cyber Security: Analytics, Technology and Automation* (195–203). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-18302-2_12.

NOTES

Stanton, Paul. (2017, March 2). Email Correspondence regarding cyber data analytics.

The White House. (2014). Big Data: Seizing opportunities, preserving values. *Washington, DC: Executive Office of the President*.

U.S. Army. (2010). *The Targeting Process* (No. FM 3-60.).

U.S. Army, U. S. (1998). *Intelligence Preparation of the Battlefield (FM 34-130)*. Department of the Army (US).

van der Heijden, T. H. C. (2012). Process mining project methodology: Developing a general approach to apply process mining in practice. *Master of Science in Operations Management and Logistics. Netherlands: TUE. School of Industrial Engineering.* Retrieved from http://alexandria.tue.nl/extra2/afstversl/tm/Van_der_Heijden_2012.pdf.

Verizon RISK Team. (2015). 2015 Data Breach Investigations Report. Retrieved from http://www.isaca.org/chapters2/Luxembourg/Documents/201510%20Digital%20Forensics%20Master%20Class/5_DBIR%202015%20-%20CLUSIL-ISACA.pdf.

Winterfeld, Steven P. (2001). *Cyber IPB*. SANS. Retrieved from https://cyber-defense.sans.org/resources/papers/gsec/cyber-ipb-103147.

Social Media—From Social Exchange to Battlefield

Beata Biały

INTRODUCTION

SOCIAL MEDIA—BEGINNINGS

When discussing the origins of social media, researchers usually start in the 1980s and the Bulletin Board Systems (BBS). They were a kind of online meeting room that allowed users to download games and other files, and leave messages to co-users. The social aspect of this exchange was pretty clear, but the interaction was rather limited and slow due to technological reasons. What is more important, the social interaction had a rather random character—people did not know who was sitting at the other end of the telephone line.

However, BBS proved a growing interest in this kind of communication and inspired other platforms to emerge from the early Internet. The big success of sites like *Classmates.com* confirmed the need for a virtual exchange of memories, ideas, and views. This time, users could enter into social interaction with precisely chosen people, and create networks of "friends", based on their common school experience. *Classmates.com* has equivalents in countries all over the world. The best example is the webpage *Odnoklasniki* (classmates), which is very popular in Russia and other former Soviet, Russian-speaking countries of Ukraine, Kyrgyzstan, Uzbekistan, and Georgia.

The second half of the 1990s has numerous examples of emerging platforms built on a similar principle, for example, *SixDegrees.com* (founded in 1997). But the real social network revolution started at the beginning of the 2000s when the *Friendster* website was launched. After just one year it had gathered a community of three million users (the first site with such a big audience). "Participatory culture" became a buzzword, enhanced by dynamic technological development. Different platforms were founded, using different "sociality" models. A particularly interesting example is *Linked-In* (2003) which is a platform for professional networking, where one's contacts were not friends

Beata Biały is a senior expert at the NATO Strategic Communications Centre of Excellence. She is a graduate of the Warsaw University in French Philology and Business Administration and completed an MBA program of the University of Illinois Urbana-Champaign. Before her civil service career, she worked as a manager in Polish media for 15 years. Beata was deputy CEO for one of the leading dailies publishing groups and deputy director of Polskie Radio Channel One. As a civil servant, she worked in the Polish Ministry of Transport where she was in charge of EU affairs, and later as director of Public Affairs Department for the Ministry of National Defence. She was responsible for creating the Strategic Communication structure in the Polish MOD and represented Poland in the NATO STRATCOM COE Steering Committee. Beata has been pursuing her passion for literature by writing books, and translating more than twenty French and English literature books.

but professional connections. It is interesting to note that *LinkedIn* has kept this particular character until the present day.

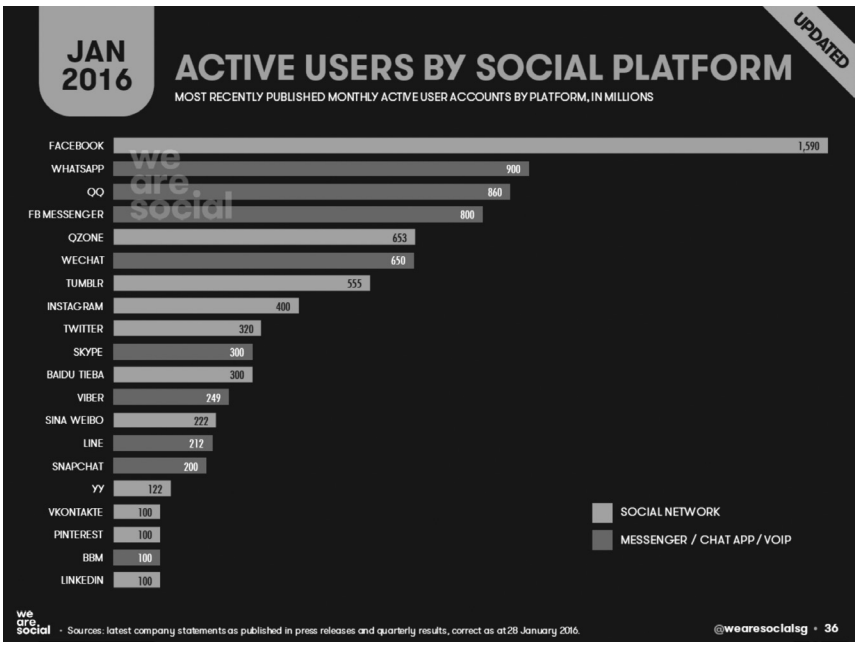
One year after *LinkedIn* was launched, Mark Zuckerberg and his Harvard University classmates, created the site *thefacebook.com* which evolved into one of the most powerful and successful social media platforms in the world with over 2 billion active users in September 2016.[1] It is user-friendly, with many easily accessible features, it has become a global brand, deserving the recognition: if you are not on *Facebook,* very likely you don't exist. *Facebook* also introduced the "like" click, which was an excellent addition, allowing users to easily express their emotions, thereby underlining the platform's social character.[2]

Created in 2006, *Twitter* focused on network conversation. Thanks to the introduction of a "hashtag" feature, users' 140-character messages can be easily tracked and grouped, which is vital on a site where every second an average of 6000 tweets are posted (about 200 billion tweets per year). Among its 313 million active users[3] (over 1.3 billion accounts) are politicians (according to some statistics, 83% of the world leaders have an account on *Twitter*[4]), journalists (24.6% of all accounts[5]), information agencies, and companies.

At more or less the same time, the online community witnessed the creation of such platforms as *Myspace, YouTube,* and *Google+,* closely followed by *Instagram, Snapchat,* and dozens of others. The recent appearance of mobile technology has strongly affected users' behavior and forced social media platforms to adapt to this new environment by introducing mobile applications. At the beginning of 2016, more than 2.3 billion people were using social media: of these, 1.9 billion users were accessing social media via their mobile phone.[6] Mobile

technology enhanced in particular the development of photo- and video-sharing platforms, such as *Instagram* or *Snapchat,* entertainment location apps (e.g. *Foursquare*), dating services (like *Tinder*), and last, but not least, direct messaging applications (like *WhatsApp*). [7]

The social media landscape is far from stable. For the last few years, companies like *Facebook, Twitter* and *Google* have been massively investing in new platforms. Big acquisitions have taken place–*Instagram* and *WhatsApp* were purchased by *Facebook, Twitter* acquired *Vine* (in October 2016, Twitter decided to close the service when it did not meet expectations), and *Google* purchased *YouTube.* The social media landscape has been evolving from relatively small local services (initially *Facebook* was dedicated exclusively to Harvard University students) to powerful companies with global reach. From more than 2.3 billion social media users (data from 2016) [8] nearly 1.6 billion have chosen *Facebook,* giving it the clear position of market leader. In the US, 79% of online adults (68% of all adults) use *Facebook,* 32% – *Instagram,* 31% – *Pinterest,* 29% – *LinkedIn,* and 24% – *Twitter.* [9]



Over time, social media platforms have become huge pools of data for advertising and marketing companies. Within the last three years, *Facebook* alone noted a 120% increase of brands placing paid promotion on the platform. Social media companies have also developed e-commerce features, allowing their users to shop directly from the social media website, following the example and advice of social network "friends". [10] Social and commercial activities have become two powerful drivers of social media platform development.

When it comes to data, it is worth dedicating a few lines to the concepts of Big Data and social media mining. As the authors of the book "Social Media Mining" state, "social media data is undoubtedly big," [11] which is only one of many challenges that must be faced by those who want to explore it. The others are the unstructured character of data, its noisiness, and social relations hidden there with friends, connections, following–followers.

These particular characteristics call for data analysis methods, which can encompass an understanding of user-generated content, including a wide range of social relations. This technique, termed social media mining, draws on the different disciplines of computer science, machine learning, social network analysis, statistics, sociology, and many others, as well as interdisciplinary concepts and theories.

Social media mining "searches for hidden patterns and relationships correlations, in addition to interdependencies that exist within large databases that the traditional information gathering methods (...) may fail to notice". [11] It aims at discovering the relations between "social atoms" (individual users), "social entities" (content, sites, networks), and interactions between the two previous categories. [13] It helps to identify communities on a social network and determine who the most important people are in a social network (the influencers).

Social media mining, draws on the different disciplines of computer science, machine learning, social network analysis, statistics, sociology, and many others.

Such analysis is useful for marketing purposes, by targeting users who are likely to effectively disseminate brand awareness and increase the reach of potential customers. In a similar way, social media mining can be used by other actors, who aim to build advocacy for their narrative. Some experts' claim that it is useful for predicting future behavior of given groups (e.g. terrorists), based on a special algorithm. [14] In any case, Big Data and social media mining are two emerging concepts with a breathtaking future.

FROM SOCIAL EXCHANGE TO SEARCHING FOR CONTENT

The appearance of social media offered Internet users an unprecedented opportunity to connect with other people. The exchange of memories, experiences, opinions, views and agendas became easy and–over time–very cheap. Suddenly, one could find former classmates and reestablish regular contact and also discover new "friends" in dynamically growing social networks. And these "friends" could come from any part of the globe with Internet access, which means from almost all over the world.

Obviously, there can be various motivations for using social networks. In April 2015, *Global Web Index* published a report presenting the reasons why people use social media (see the next chart). Among the top ten, reason number one is clearly "social"—"to stay in touch with what my friends are doing". There are also other responses on the list, like sharing one's opinion or details of one's private life, sharing pictures or videos, networking with people, meeting new people, and being there "because a lot of my friends are on it"—all of these show high social motivation. But it is worth noting number two on the list—"to stay up-to-date with news and current events", which has nothing to do with the social character of "social networking services" (as it was stated in the survey question). Looking for information, not necessarily about friends, but for information in general, has been a growing trend among social media users. Social networks are more and more considered a source of content, although this content is generated by the users themselves.

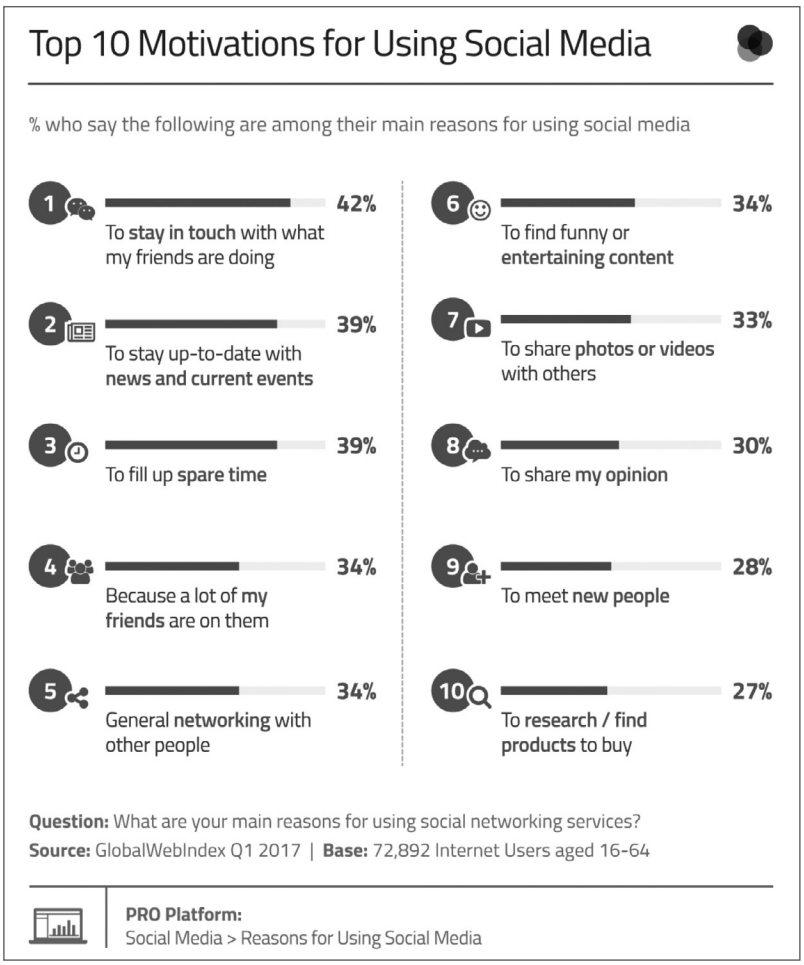


Figure 1. Source: http://www.globalwebindex.net/blog/top-10-reasons-for-using-social-media

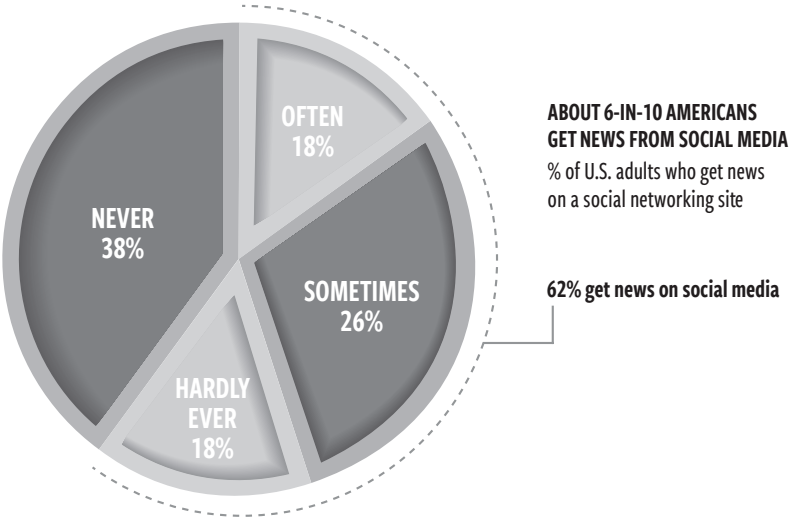


Figure 2. Source: Survey conducted January 12- February 8, 2016. "News Use Across Social Media Platforms 2016" **Pew Research Center**

This trend was also observed by researchers from SWOCC (research organization linked to the department of communication studies at the University of Amsterdam). Their study, carried out in 2016, showed that users' perceptions of social media had changed considerably. Some platforms are perceived as being less "social", and more "informative" (e.g. *Twitter*). Other research from 2016, conducted by Pew Research Center, concludes that 62% of US adults are getting their news from social media. The growing trend seems obvious, in 2012, this number was 49%.

Although it would be risky to say that social media platforms have become a direct competitor to mainstream media, their role in the flow of information is prominent. What is more, they have become a source of content for traditional media. Information agencies and journalists establish their *Twitter* or *Facebook* accounts not only to disseminate their message but also to hunt for news posted by other social media users. In such a way, information generated by a "grassroots journalist" [15] can obtain an unexpectedly large reach. This can become problematic if the news appears to be inaccurate or simply fake. An excellent example of such misinformation is the "Senator Cirenga case"; a sensational post on the *Facebook* account of a non-existent Italian senator, which was used and covered by several newspapers, and turned out to be untrue. [16]

The above-mentioned example shows how challenging and risky it is for an Internet user to consider social media a source of information. Easy access, the possibility of anonymity, and no gatekeepers are a dangerous mix. In traditional media, journalists are supposed to observe the rules of the profession, and editors check if an article meets the standards of accuracy, and reliability, then decide if it can be published. On social media, anybody can become a 'journalist' and, anything can become 'news'.

FROM SOCIAL EXCHANGE TO BATTLEFIELD

Over the last six years, the number of social media users increased more than twofold (0.97 billion in 2010 to 2.34 billion in 2016 [17]). These numbers, together with changing usage patterns, have made social media a very attractive communication channel. Low access cost, various target audiences, global reach, and the unprecedented speed of information flow—all these factors encourage different actors to use social media for their purposes. Marketing experts discovered its potential very quickly and placed social media in the heart of their promotion campaigns. But they were not the only ones.

Because, apart from its monetizing potential, social media has also become an excellent channel to mobilize support, disseminate narratives, wage information operations, or even coordinate military operations in the real world. States and non-state actors have started to extensively use social media to influence perception, beliefs, opinions and behaviors of their target audiences. Although social media has been a very useful communication channel to support legitimate and worthy actions (such as humanitarian aid in disaster areas), it is more and more used for other, far less noble aims. The chart below, from Dr. Rebecca Goolsby's article on social cyberattacks [18], shows how social media conversations can be used for different purposes.

ON CYBERSECURITY, CROWDSOURCING, AND SOCIAL CYBERATTACK

CRISIS RESPONSE	COMMUNITY DIALOGUE	INFLUENCE	SOCIAL CYBERATTACK
Disaster Relief	Anti-Propaganda	Propaganda	Crowd Manipulation
Humanitarian Assistance	Rumor Squelch	Rebellion Cry	Hysteria Propagation
Crisis Monitoring	Community Outreach	Hate Messages	
PROMOTES:	**PROMOTES:**	**PROMOTES:**	**PROMOTES:**
Order and Discourse	Discussion Expansion	Special Point of View	Chaotic Mass Behavior
Cooperative Behavior	Spread of Verifable Information	Bandwagon Effects	Escalation of Rumor
Information Sharing		Conflict and Argument	Confusion, Panic and Violence
		Mass Protests	

Figure 3. Source: Office Of Naval Research Arlington VA http://www.dtic.mil/get-tr-doc/pdf?AD=ADA580185

The recent conflicts in the Middle East and Ukraine demonstrated that social media could be a very useful means to support military operations. Since then, it has been exploited to such an extent that it seems justifiable to call social media an information confrontation battlefield. Obviously, there are many different ways of using social media

for supporting military objectives. Tomas Elkjer Nissen identifies six of them: intelligence collection, (geo-) targeting, cyber operations, command and control, defense, and psychological warfare (inform and influence). [19]

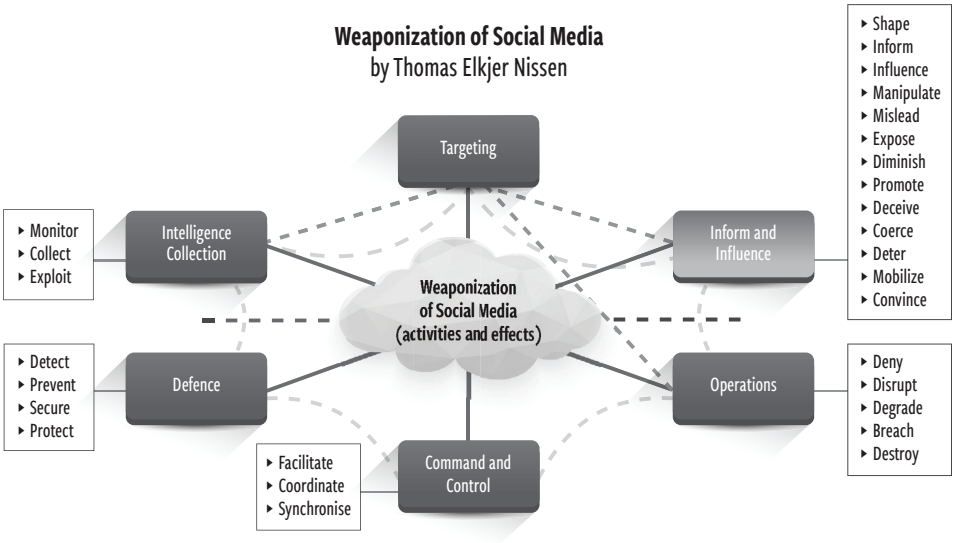


Figure 4. Source: Social Media as a Toll of Hybrid Warfare, NATO Strategic Communications Centre of Excellence, Riga, July 2016, p. 11

Intelligence collection—monitoring and analyzing the information that can be found in social networks, such as social media profiles, specific social media communities, conversations' content and temperature. The collected information can be useful for target audience analysis, which is crucial for planning information operations. It is also helpful for planning kinetic activities on a given theater.

(Geo-) targeting—exploring virtual reality (in this case, social media) to identify targets for military operations carried out in the real world. Such analysis uses geo-tagged pictures, the content of users' conversations, and geo-located data. The risk of geo-targeting has been recognized early-on by different actors. For example, in 2014 the Islamic State of Iraq and the Levant (ISIL) or Daesh prohibited its *Mujahideen* from switching-on the original *Twitter* geo-tagging function. [20]

Cyber operations—breaching passwords, hacking social media or email accounts, altering the content or making some accounts unusable. Cyber operations can be carried out to collect intelligence, prevent other actors from using social networks, sow disinformation and confusion. The picture below shows an example from April 23, 2013 when the Associated Press *Twitter* account was hacked to disseminate a false claim of explosions at the White House. [21]

Figure 5. Source: Twitter @AP The Associated Press

The temporary suspension of the AP account was only a minor effect of this operation. The violent reaction of the Dow Jones Index (see the chart below) is a perfect illustration of serious impact.

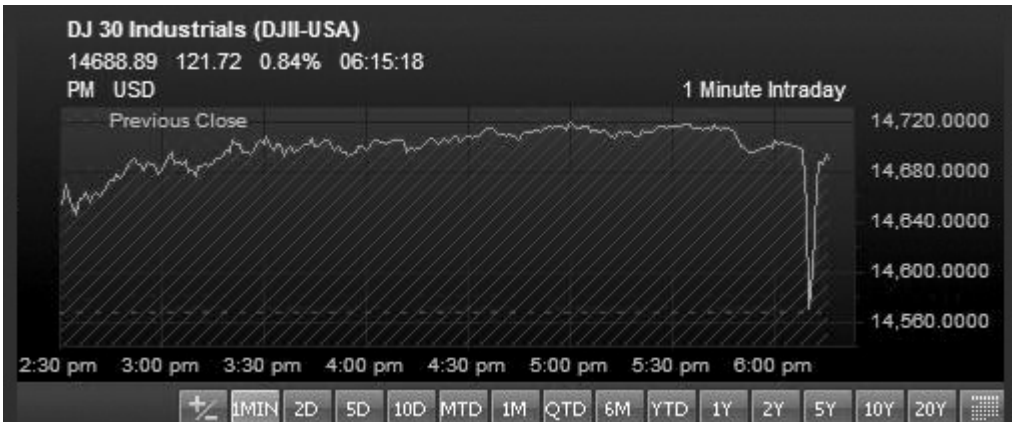


Figure 6. Source: http://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured

Command and Control (C2)—using social media platforms for internal communication and coordination. Depending on their objectives, different actors can use more or less open networks to synchronize their operations. An especially interesting example is the *PlayStation* game network used by Daesh for coordination of its actions.[22] Obviously, different social media platforms represent varying levels of security. For this reason, actors like terrorist organizations often choose closed networks for their communication. For example, Daesh uses the adaptive structure of its network to defend it against possible infiltration or external influence.

Defense–all kinds of activities whose objective is to protect a given social network against being penetrated by adversaries. This includes such activities as encryption, anti-tracking, IP concealing, or the above-mentioned use of adaptive structures. Joseph Shaheen describes this technique as a DEER process: Dissemination (of public propaganda); Deletion or suspension of the account (by an adversary); Evolution of (network) structure or methods; Expansion of influence or methods; Replenishments of accounts and resources. [23] Defense also means making social media users aware of the risk they encounter by communicating via different social media platforms. An example of such "instruction" is the guide circulated by Daesh in January 2016 (see the chart below) giving Daesh followers' clear indications of platforms considered "safe" and "unsafe". [24]

Figure 7. Source: The Wall Street Journal (SITE Intelligence Group)

Psychological warfare (inform and influence)–using social media as the channel for disseminating messages whose objective is to influence (change) target audiences' opinions, beliefs, perceptions, and behaviors. It means achieving some military effect in the cognitive domain using misinformation (including disinformation) and propaganda.

Without minimizing the importance of the first five above mentioned hostile activities, we will examine closely the last one–psychological warfare on social media.

SOCIAL MEDIA—INFORMATION WARFARE BATTLEFIELD

Psychological warfare on social media can take different forms—overt or covert, depending on the target audience and objectives. Overt methods consist of acting via official social media accounts and channels. Covert methods involve creating false accounts, using social media trolls (called by some experts "hybrid trolls [25]) or bots, addressing closed social networks. The second category of activities is abundantly explored by those actors who do not observe democratic legal and ethical standards, such as terrorists or authoritarian states. On the other hand, there are democratic countries and organizations acting according to democratic values and principles, which exclude these kinds of covert activities carried out in peace time.

The social media landscape has been evolving from relatively small local services to powerful companies with global reach.

For example, the NATO Allied Joint Doctrine for Psychological Operations states that "PSYOPS may be conducted ... across the full spectrum of military operations." [26] In the same document, Information Operations are defined as "a staff function that analyzes, plans, assesses and integrates information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries, and North Atlantic Council (NAC) approved audiences in support of Alliance mission objectives." [27] Ergo, psychological operations may only take place in the context of military operations, and the target audiences need to be approved by the highest NATO decision-making body.

In the case of terrorist organizations or authoritarian states, the boundaries between war and peace are often blurred, and covert influence activities are used even if no war has been officially declared. This kind of approach lies at the basis of Russia's information warfare theory. As Dr. Jolanta Darczewska at the Polish Centre for Eastern Studies remarked, this theory had been built in opposition to the western concept of cybersecurity. The latter is mostly about using technology for military and intelligence purposes. Russia's theory understands information warfare as "influencing the consciousness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as 'information weapons'". [28] Military and non-military orders are muddled up, and discrepancies between "civilizational systems" are a sufficient justification for carrying out psychological operations in the information space.

In information warfare, actors use different tactics. Ben Nimmo, Information Defense Fellow at the Atlantic Council Digital Forensic Research Lab, singles out four such methods, situating them in the context of the Ukrainian conflict, and calling this set of tactics the "4D Approach". [29] The four Ds stand for dismiss, distort, distract, and dismay.

Dismiss–undermining the opponent, denigrating him, or simply denying uncomfortable facts. An interesting example of this tactic is the use of the term "Russophobe" by Kremlin supporters. If somebody criticizes Russia, he/she automatically becomes Russophobe, which means ignorant, one whose opinions are grounded in prejudices, and therefore not worth noting.

Figure 8. Source: Sputnik's Twitter account

Distort–twisting facts, misinterpreting and putting them out of context, or last but not least, producing a partly or totally false version of reality. This tactic is abundantly used by Kremlin partisans, and its extreme form is the "rewriting of history" extensively present in social media messages posted by pro-Russian users. Another example of this tactic is Daesh propaganda videos disseminated on *YouTube,* which aims to convince the Islamic audience how expertly organized is the "Islamic State's" healthcare, and how much the "ISIL" cares about its citizens and supporters. [30]

Distract–turning the audience's attention away from the actor's activities, and focusing it on activities of the opponent. For example, pointing out that NATO is an aggressive organization that is sending troops all over the world, or accusing the US of expansionist policy when the social network discussion is about Russian annexation of Crimea.

Dismay–frightening the target audience with verbal warnings or disturbing pictures and videos. The Kremlin has mastered this method and uses it broadly both towards the internal and international audience. Kremlin statements about the "adequate response" that will be given by Russia to NATO's or US "aggressive policy" are willingly taken up and repeated in social network discussions. Another example is Daesh propaganda videos showing crucifixions or beheadings of the "unfaithful".

Figure 9. Source: Twitter

Figure 10. Source: Twitter

Although Ben Nimmo assigned the 4D Approach specifically to Russia, these tactics are also used by other actors, and social media is a very convenient platform for their application. Internet users who more and more frequently consider social media as their main source of information are an attractive target for those who do not hesitate to manipulate or falsify facts and present their version of reality, supporting their particular agenda. To increase effectiveness, they use a variety of techniques and methods, examined below.

METHODS AND TECHNIQUES

One of the most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency and availability 24/7. The conversations in social networks can be conducted almost in real time, and—as has already been mentioned—the quantity of messages (posts) appearing on the user's screen can make his/her head swim. This is a big challenge for somebody who wants their message to be visible. Therefore, one of the techniques used by different actors on social media is posting **automatically generated content** or **human generated content which is automatically spread through fake accounts using bots and apps.** Within the last few years, the number of these social media accounts has noticeably increased—according to different studies, at least 8 percent of *Twitter* accounts [31] and between 5 and 11 percent of Facebook accounts are bots. [32] According to *The ISIS Twitter Census,* 20% or more of all Daesh tweets are created using bots or apps. [33] Although social and IT scientists have been inventing more and more effective tools for the detection of bots, the other side has not remained passive with bots becoming more sophisticated, more 'human', and therefore, difficult to discover and eliminate.

Low access cost, various target audiences, global reach, and the unprecedented speed of information flow—all these factors encourage different actors to use social media.

It is important to note **the extensive use of mobile technology** to convey messages directly to users. The mobile revolution mentioned at the beginning of this article creates a great opportunity for those who want to effectively spread their message. The mobile app *Dawn of Glad Tidings* was distributed by *Daesh* to supporters in 2014 and enabled them to use their *Twitter* accounts to automatically tweet *Daesh*-related content. This was the first attempt by the organization to use a mobile app for the automatic distribution of its messages. Although it was closed down by *Twitter* pretty quickly, it was able to mobilize 40,000 people to sign up for the app. Currently, a new Android app is in place allowing the *Daesh* radio *Al-Bayana* to broadcast outside the boundaries of their operating territory. In May 2016,

a new app was developed to teach the alphabet to children, but one can find a large number of references to weapons and *jihad.* [34]

Another technique used to increase the exposure of a given narrative on social media is **trolling.** However, it is important to note the fundamental difference between a "classic" internet troll and a "hybrid" troll. The first category has been present in digital media from the very beginning and designates a particular kind of social media user who, for purely personal reasons (frustration, unhappy life, and psychological problems), tries to disrupt social network conversation by offending other users, provoking, and posting unpleasant comments or comments out of context. The other one is a kind of social media warrior, hired by a state or a non-state organization for supporting this organization's cause and executing its agenda. [35] These "information *spetsnazes*", as they are called by one of the eminent Russian theorists of information warfare, Igor Panarin [36], are tasked to post comments to either promote the narrative of their patron or to destroy the narrative of his opponents. They overwhelm social media with a huge volume of posts, using different manipulative techniques and methods which have enabled researchers to discern a couple of interesting categories of hybrid trolls: "bikini troll", "Wikipedia troll", "aggressive troll", "attachment troll", and "conspiracy troll" (also called "blame the US troll"). [37] The good news is that social media users are not defenseless against hybrid trolls, and a minimum level of awareness and practice can help to detect and expose them. In one of its reports, the NATO Strategic Communications Centre of Excellence published an "Internet Trolling Identification Tutorial" [38] presenting a four-step approach which can help in countering hybrid trolls' activity.

The most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency and availability.

Trolling (especially "attachment trolls") **can also be used for conducting cyber operations,** such as intelligence collection. The Latvian Information Technology Security Incident Response Institution (CERT) discovered that pro-Russian trolls were using the comments sections of Latvian web portals to disseminate propaganda and encourage other users to click on web links containing spying malware. [39]

An effective method of increasing the impact of a narrative or specific messages is the **coordinated use of multiple channels**—open and closed. The communication goes through public conversation platforms, such as *Twitter,* and within closed networks, such as encrypted messengers or—as it was mentioned earlier—even via *PlayStation Network* which is extremely challenging for decryption, and more difficult to track than *WhatsApp.* Documents leaked by Edward Snowden in 2013 revealed that the NSA and CIA attempted

to infiltrate terrorist conversations by taking part in games like *World of Warcraft.* [40] Public networks are mainly used for spreading propaganda or misinformation, while closed social networks may be an efficacious channel for coordination of activities (C2), recruitment and the mobilization of support.

An interesting mutation of the above-mentioned technique is the Kremlin's **cross-media communication approach** broadly used in the Ukrainian conflict. The idea consists of feeding the mainstream media with information, mostly fake, posted on social media or—vice-versa—disseminating materials made by pro-Kremlin media (e.g. TV channels controlled by Kremlin or pro-Kremlin websites) via social media conversations. A striking example of this method is the case of "Doctor from Odessa", an alleged emergency physician who described on his *Facebook* account a dramatic story of his fight to save wounded civilians. In the post, the "Doctor from Odessa" he depicted, in a very emotional way, the cruelty of pro-Ukrainian extremists who stopped him from tending to his patients. Although bloggers investigating the "Doctor's" case discovered that such a person did not exist, and the *Facebook* account was blocked, the story immediately became very popular and was covered by the media. [41]

For spreading a given message even further, the cross-media communication approach can also be combined with other techniques, such as the use of botnets. And last, but not least, it has become a general rule to integrate pro-Kremlin online media: Russia Today, and Sputnik with social media (*Twitter,* etc.).

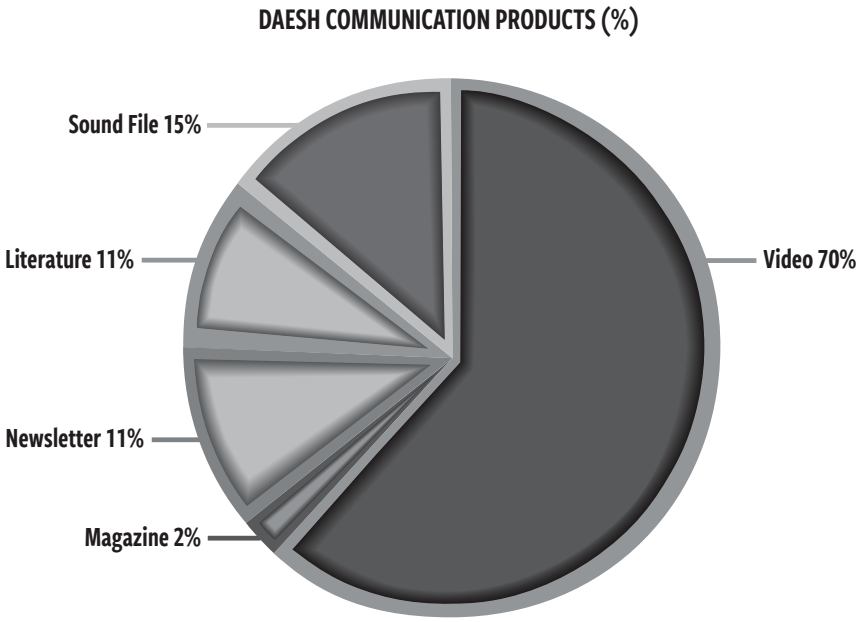


Figure 11. Source: NATO StratCom COE report The DAESH Strategic Narrative, June 2016

To be effective on social media, **attractive, memorable,** and **emotional content** is essential. Different actors, such as Daesh, understand the **primacy of visual content** over verbal messages; it is much easier to capture the audience's attention and achieve its engagement when using images—the most engaging posts on *Facebook* are photos. [42] The majority of *Daesh* products are pictures, videos, games, and music.

An interesting example of such content is *Nasheeds,* chants which are a mixture of religious and social narratives inspiring Daesh supporters. *Nasheeds* are available on the *YouTube* "Best *Nasheed* Channel", and have recently started to appear in different European language versions. [43]

Visual content has two major functions - to impress or to dismay. It rarely has a purely informative character. It is also interesting to note the **significant role played** in psychological warfare **by humoristic drawings and pictures.** A famous example is the picture montage tweeted by the Russian deputy prime minister, Dmitry Rogozin (see below), illustrating the "different values and allies" (original tweet: *У нас разные* ценности *и союзники*) of Russia and the USA, which became rather popular (retweeted 2500 times).

Figure 12. Source: Dimitry Rogozin's Twitter account

CONCLUSIONS: WHAT CAN WE DO?

Social media is one of the most dynamically developing communication platforms. It has been subject to many significant changes, evolving from small, scattered, local community websites, to consolidated companies with global reach. Social media has also witnessed a leap into mobile technology, which has had a tremendous influence on human behavior, including social media usage patterns. Last, but not least, over time, users motivations to participate in discussion on social media have also changed. The purely "social" motivation has been gradually replaced by other motivations, such as the search for information, which has situated social platforms much closer to traditional media.

Social media has also witnessed a leap into mobile technology, which has had a tremendous influence on human behavior.

A dramatic change took place in this information environment that can be called the weaponization of social media, which means transforming social networks into a field of hostile information activities carried out on target audiences in the gray zone between peace and war.

Thanks to its exceptional features, such as global reach, high accessibility, low cost, huge volume and speed of information exchange, and—to some extent—user anonymity, social media is attractive to multiple actors with hostile agendas. Paradoxically, what has been its big advantage, has become a considerable weakness. Platforms which—by definition—were born to be "social", have witnessed a great number of activities having a clearly anti-social character.

Hence, it seems highly justifiable to call social media a battlefield on which an intense fight for hearts and minds is taking place. It is a battlefield where we can observe different military strategies and tactics, such as deception, disinformation, propaganda, threatening opponents, mobilization of supporters, and coordination of actions. The development of technology plays a prominent role, making all those activities easier and more effective. Human actors are extensively assisted or even replaced by bots and apps, and the content (message) becomes—thanks to the development of multimedia—more and more attractive.

The question then arises as to what the democratic world can do to counter hostile activities on social media, and in the information environment in general, given that the adversary does not observe the same legal rules and ethical principles as a democracy, and does not share democratic values. Moreover, the adversary is cunning, fast, flexible and adaptive, due to the particular character of its organization—authoritarian (Kremlin) or dispersed (Daesh), whereas democratic countries and institutions are obliged to follow specific procedures with lengthy decision-making processes.

The challenge is enormous, but the future is not lost. Observation of the social media environment and the activities of "bad actors" enable us to formulate a few key recommendations.

Be present on social media with attractive, well-tailored content. It is a vital part of the information environment, and it should be considered as an obvious element of communication campaigns. Instead of choosing platforms, it is wiser to choose target audiences, and to follow them—they have already chosen their platforms.

Use what technology offers. Our adversaries use it effectively, creating attractive content and disseminating it via multiple channels. "Think mobile" is not just a catchy slogan. Neither is "cross-media activity". But do not forget that "social media is about sociology and psychology more than technology" [44].

Advance your own narrative and develop attractive branding. A well prepared offense is usually a more certain path to victory than defense. When promoting your narrative, be consistent and credible.

Build your brand and narrative advocacy. Find credible voices within the target audiences that can speak for you. Humanitarian organizations' experience with crowdsourcing can serve as a very useful model.

Immunize your audience against psychological operations. It is vital to raise citizens' awareness of the influence activities used by our adversaries. There are two main lines of defense: education and exposure of hostile activities. Education gives citizens (starting from relatively young age) basic knowledge about media and social media that helps build critical thinking and fact-checking habits. Exposure of hostile activities requires tracking online deception, manipulation and disinformation, and neutralizing it with the truth. Because however lofty it may sound, truth is a powerful weapon.

NOTES

1. http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

2. http://www.digitaltrends.com/features/the-history-of-social-networking/.

3. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

4. https://www.brandwatch.com/blog/44-twitter-stats-2016/.

5. Ibidem.

6. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 13. All reports of NATO StratCom COE can be found here: http://www.stratcomcoe.org/publications.

7. Ibidem, 13.

8. Special Report: *Digital in 2016,* http://wearesocial.com/uk/special-reports/digital-in-2016.

9. http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

10. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 9.

11. Reza Zafarani, Mohammad Ali Abbasi, Huan Liu, *Social Media Mining,* Cambridge University Press, April 20, 2014, http://dmml.asu.edu/smm/SMM.pdf.

12. Daniel Armstrong, *Exploring Social Media's Influence during Conflict and Crisis,* Grounded Curiosity, November 2016, http://groundedcuriosity.com/exploring-social-medias-influence-during-conflict-and-crisis/#_ftn37.

13. Reza Zafarani, Mohammad Ali Abbasi, Huan Liu, Op. Cit.

14. Catherine Caruso, *Can a Social-Media Algorithm Predict a Terror Attack,* MIT Technology Review, June 16, 2016, https://www.technologyreview.com/s/601700/can-a-social-media-algorithm-predict-a-terror-attack/.

15. The concept of grassroots journalism was exquisitely developed by Dan Gillmor in his book *We the Media, grassroots journalism by the people, for the people,* O'Reilly Media, Inc., 2004.

16. https://www.weforum.org/agenda/2016/01/q-a-walter-quattrociocchi-digital-wildfires?utm_content=buffer-259d4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

17. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

18. Rebecca Goolsby, *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack,* http://www.stratcomcoe.org/rebecca-goolsby-cybersecurity-crowdsourcing-and-social-cyber-attack.

19. Report *Social Media as a Toll of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 13.

20. Report *Network of Terror: How DAESH uses adaptive social networks to spread its message,* NATO Strategic Communications Centre of Excellence, Riga, December 2015, 9.

21. http://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured.

22. Report *Social Media as a Toll of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 17.

23. Report *Network of Terror: How DAESH uses adaptive social networks to spread its message,* NATO Strategic Communications Centre of Excellence, Riga, December 2015, 21.

24. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 32-33.

25. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 10.

26. AJP – 3.10.1, Allied Joint Doctrine for Psychological Operations, 2014, section IV – *Principles of PsyOps.*

27. Ibidem, section III - *PSYOPS within strategic communications and information operations.*

28. Jolanta Darczewska, *The Anatomy of Russian Information Warfare, the Crimea Operation – a Case Study,* Point of View, Centre for Eastern Studies, Warsaw, May 2014, 11-12, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

29. http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

NOTES

30. You can watch one of these propaganda films here: https://www.youtube.com/watch?v=hiY7JFadLm8.

31. *Twitter Has Stopped Updating Its Public Tally Of Bots,* William Alden, *BuzzFeed,* November 10, 2015, https://www.buzzfeed.com/williamalden/twitter-has-stopped-updating-its-public-tally-of-bots?utm_term=.qyl1lVP6D#.pbYRR3mJZ.

32. *Facebook estimates that between 5.5% and 11.2% of accounts are fake,* Emil Protalinski, The Next Web, http://thenextweb.com/facebook/2014/02/03/facebook-estimates-5-5-11-2-accounts-fake/.

33. Report *Social Media as a Tool of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 37.

34. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 34.

35. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 10.

36. Jolanta Darczewska, *The Anatomy of Russian Information Warfare, the Crimea Operation – a Case Study,* Point of View, Centre for Eastern Studies, Warsaw, May 2014, 16, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

37. For more information see the Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016.

38. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 42.

39. Report *Social Media as a Tool of Hybrid Warfare,* Strategic Communications Centre of Excellence, Riga, July 2016, 31.

40. Appropriate fragments of the leaked documents can be found here: http://gawker.com/nsa-and-cia-spied-on-world-of-warcraft-other-online-vi-1479458437.

41. Report *Analysis of Russia's Information Campaign against Ukraine,* NATO Strategic Communications Centre of Excellence, Riga, July 2015, 23.

42. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 23.

43. Report *Daesh Recruitment, How the Group Attracts Supporters,* NATO Strategic Communications Centre of Excellence, Riga, November 2016, 23-24.

44. Brian Solis' quotation used in the article by Nicole Matejic *3 things Anthony Robbins reminded me about communication:* http://www.infoopshq.com/2016/10/02/3-things-anthony-robbins-reminded-me-about-communication/.

Operationalizing Cybersecurity — Framing Efforts to Secure U.S. Information Systems

Dr. Dawn Dunkerley Goss

ABSTRACT

Society has become utterly dependent on information systems (IS) to power everyday life. While this seismic shift has taken place, the security of those IS and their consequential information assets has not taken a front seat alongside innovation, resulting in breaches of trust and loss of corporate goodwill. Organizations are struggling to find an effective approach that encompasses not just technical aspects of cybersecurity, but also improves people and processes. This article will define, discuss, and operationalize the technical, semantic, and effectiveness aspects of cybersecurity and their application into the organizational construct.

INTRODUCTION

IS power an increasing amount of modern infrastructure; from online banking to the social networks connecting disparate friends and family, this reliance on computing systems is unprecedented and can be expected to grow into the future. However, the value of the information itself outpaces the value of the systems storing the information. When calculating the damage created by a breach of cybersecurity, research has shown the greatest damage to be the loss of information resources and their resultant strategic advantages. [1] [2]

Even while organizations are beginning to fully realize the value of their IS and information assets, cybersecurity incidents do occur, and with potentially significant losses. These losses are of both a monetary nature, as well as compromises to information assets. While it can be difficult to determine the full extent of losses suffered through cybersecurity exploits [1] [2] [3], threats certainly have been realized at the corporate, state, and federal levels. The sheer losses borne by organizations fundamentally underline the problems that face corporate entities and nation-states as their infrastructures become increasingly technological and enemies become increasingly sophisticated in their attack techniques.

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

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

Public and private enterprises have developed a number of methodologies to combat threats to their IS and associated information assets. For example, the U.S. Department of Defense has adopted the National Institutes of Standards and Technology (NIST) Risk Management Framework (RMF), a checklist-based approach leading towards an authoritative approval to connect. While these prescriptive, checklist-centric approaches have various sets of controls, they have a common aim: providing a level of security that counterbalances the threats to the IS.

FRAMING AN APPROACH

Many have argued the definition of *information*, perhaps to the unfortunate consequence of this phenomenon containing a bulk of definitions proposed only to serve the narrow interests of those defining them.[6] More recently, literature has placed information into a framework alongside data, knowledge, and wisdom. The data-information-knowledge hierarchy describes data as "a set of signs formulated in a structure and governed by formal rules being processed and interpreted to form information".[7] This information is transformed into knowledge as it is combined with context and personalized into organizational "know-how".[8] Kane (2006) suggested that data, information, and subsequent knowledge are indistinct entities along a single continuum.[9] This is crucial in the context of this research, as the end benefits provided by knowledge synthesis and exploitation are impossible if the information itself is irretrievable, unusable, or without value.

The concept of the *information system* has similarly been debated with varying outcomes. While many see the domain and corresponding terminology in technical terms only[10], IS surpasses a broader swath of understanding than this narrow definition belays. Understanding what encompasses an "infor-

mation system" is fundamental to understanding its role in the organizational context. Does an IS consider both the technology and the personnel using that technology? Does it also consider the organizational constructs enabling both the underlying infrastructure and the personnel through policies and procedures? O'Donovan and Roode (2002) suggested that IS cannot only be concerned with the exploitation of technology but must also consider the effects of technology and the changes—both challenges and opportunities—it can bring. [11]

Many researchers have attempted to define IS on the basis of levels representing these inherent contradictions. Shannon and Weaver (1949) described an IS as having three distinct levels: "technical", defined as incorporating the production of the information; "semantic", defined as the success in conveying the intended message to the receiver; and finally, "effectiveness", described as the level of effect the information actually has on the receiver. [12] Shannon and Weaver clearly believed that the technical must co-exist alongside the socio-organizational aspects to fully encompass the definition of an "Information System". This article will consider the previous passage and adopt the definition presented by Liebenau and Backhouse (1990) defining an information system as an aggregate of information handling activities at the technical, formal and informal levels of an organization. This definition provides an effective representation of the various aspects of consideration within an IS: the technical level includes the information technology present within the organization, the technology is often mistaken as the IS itself. The formal level includes the bureaucracy, rules, and forms concerned with the inter-organizational and the intra-organizational use of information. Finally, the informal level includes the organizational sub-cultures where meanings are established, intentions understood, beliefs, commitments, and responsibilities are made, altered, and discharged. [13]

While organizations are beginning to realize the value of their IS and information assets, cybersecurity incidents do occur, and with potentially significant losses.

Anderson (2003) argued that many definitions of *information systems security* described the processes or concepts adopted towards IS security (hereafter referred to as cybersecurity) without defining the end state—again considering the means without the end. [14] Many definitions of cybersecurity focus on the concepts of Confidentiality, Integrity, and Availability, the so-called CIA Triad, while other research adds attributes such as authenticity and non-repudiation. However, this research is based on the perspective presented by Anderson (2003) that, while these individual notions are worthy goals to be achieved, they are not the "end state" of a cybersecurity program and should not be viewed as such.

Anderson (2003) further argued that a proper definition of cybersecurity must be both flexible and attainable, and support the organizational context in which it is implemented. This passage will adopt the definition of cybersecurity adapted from Anderson (2003) and Dunkerley and Tejay (2012) of "a well- informed sense of assurance that information risks and information security controls are in balance." [15] This definition promotes the concept of balance within an organizational cybersecurity program that considers both the security of the IS and its concomitant data while not tossing the business objectives out the door at their expense. It is key to remember that this definition may differ widely between organizations and sectors (public versus private), based on the sensitivity of the information assets and the nature of the organization itself. For example, healthcare organizations will have a different set of requirements than a military organization and must adjust accordingly.

PAST EFFORTS IN FRAMING

TECHNICAL CYBERSECURITY

Technical research has dominated the field to date. [16] Studies and resultant frameworks have been developed to determine the proper set of technical controls that will secure an organization's IS infrastructure. Some examples of these studies include: encryption, focused on security of the IS's data assets [17] [18]; digital signatures that assure non-repudiation [19] [20]; application security, designed to strengthen the applications hosted by the IS [21] [22] [23]; finally, hardware infrastructure including intrusion detection and firewalls. [24] [25] [26] [27] [28]

When calculating the damage created by a breach of cybersecurity, research has shown the greatest damage to be the loss of information resources.

Technical research has largely focused on protecting infrastructure by facilitating the classic CIA (Confidentiality, Integrity, and Availability) triad, while occasionally interspersing theories developed within the social, criminological, or behavioral domains. CIA has become such a cornerstone of cybersecurity that while a host of other factors have been proposed, such as responsibility, trust [29], non-repudiation and authenticity [30], the CIA triad is the fundamental core of the domain. Most frameworks and policies have been based on the pursuit of these fundamental principles, and many studies assume that achieving the CIA of an organization's assets is the end game of a cybersecurity program. [29] [30] [31] [32] [33] [34] [35] [36]

Anderson (2003) argues, however, that true cybersecurity is not only CIA, and that to fully secure an organization, there must be metrics accompanying the CIA principles.

Further, Anderson urges metric development, not only for CIA but also for the quantification of the value of the cybersecurity program and how the program provides the organization and its stakeholders a "well assured sense of assurance" (p. 313).

ANALYSIS AND MANAGEMENT OF RISK

Risk management is often part of an organizational construct that includes governance and policies [37]. This harkens back to the concept of balance: within a cybersecurity program, the security risks of the organization must be considered alongside the organizational strategies to maximize gain while minimizing loss [38]. However, this strategy assumes that the organizations understand the risks to their organization, which research shows is rare; in fact, it appears that more organizations would be glad to accept risk management theories if they understood the inherent risks to their organization and how to implement a risk management program [39].

Risk management research assumes that a clear analysis and understanding of risks is critical to achieving effective security within an organization; the goal, then, of risk analysis is to help management make informed decisions about investments and to develop those risk management and cybersecurity policies [37]. To properly conduct this process, the organization must then consider the constraints in place inherent to the organization [40]. Risk analysis methodologies measure risk in one of two ways: either as the probability of a negative outcome, or a product of the probability of a negative outcome due to a threat and the probability that the corresponding control will fail to eliminate the threat [41] [42] [43]. To that end, many IS risk analysis methodologies are prevalent across academia and industry. These include quantitative method (e.g., expected value (EV) analysis [41] [42] [43]), stochastic dominance approach [45], Livermore Risk Analysis Methodology (LRAM) [42]), qualitative methods (e.g., scenario analysis, questionnaire, and fuzzy metrics), and tool kits (e.g., Information Risk Analysis Methodologies (IRAM), the CCTA Risk Analysis and Management Method (CRAMM) [40], National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-37, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method [46]. In turn, risk analysis methodologies have evolved from more checklist-based approaches [37] to include more sophisticated theories such as Theory of Belief Function (e.g. [40] and finally, strategic conceptual modeling approaches [47].

> Studies and resultant frameworks have been developed to determine the proper set of technical controls that secure an organization's IS infrastructure.

An effective analysis of risks requires an understanding of what threats are present. A number of studies have attempted to classify threats into various taxonomies, to include categorical [48], results-based [49] [50], empirical data-based [51] [52], matrix-based [53] [54], and process-based [55].

Risk analysis methodologies have been criticized for a variety of perceived weaknesses [56], including over-simplification [57], lack of a scientific approach [58], lack of lucidity [59], and the random nature of actual attacks [60]. Further criticisms have been leveled at functionalist approaches to risk analysis, which claim that organizations over-rely on risk analysis as a predictive model without fully considering other fundamental factors, as the user's behavior [58] [61]. Again, the user is key: research has shown that human risk taking occurs not only through cybersecurity incidents [62] but also through poor decision making when an incident occurs [63]. Again research shows that when the technical aspects are considered without a full understanding of the psychological and cultural variables, the results are not as useful [64]. All things considered, risk analysis is considered valuable by many researchers—even those critical of the current methods—as a process containing merit, if only for providing order to chaos and helping to gain management support for the cybersecurity program [58].

Cybersecurity evolved with a reliance on checklists and other "one-size-fits-all" measures aimed at finding the specific minimum control set that will best protect information systems.

Risk analysis is just one part of the risk management process that has been considered; after threats have been assessed and risks determined, the management of those risks is key—with the ultimate goal maximizing gain for the organization while minimizing loss [38]. This is a long-term process with outputs that feed directly into a healthy governance model, with the expectation that senior management must fully understand organizational risk in order to incorporate it into the strategic outlook. To this end, risk management is not a tool for reflection; risk management, when executed properly, directly contributes to organizational effectiveness [65], should be proactive innature [38] and should be integrated into business processes [66].

Risk management involves a calculated application of selected controls. Straub and Welke (1998) posited that, based on the extant research, controls would fall into one of four distinct categories: deterrence, prevention, detection, and recovery. Studies suggesting controls often use General Deterrence Theory to provide explanations their proposed method will be effective at controlling risk. A number of methodologies have

been developed to facilitate risk management implementation including the Business Process Information Risk Management (BPIRM) approach [35] [66], the Fundamental Information Risk Management (FIRM) methodology [67], and the Perceived Composite Risk (PCR) metric [68].

However, in spite of the research conducted, the methodology followed, and the controls implemented, researchers have argued that there will always be a residual amount of risk to an IS, regardless of the actions taken or decisions made [39] [38] [40] [68]. Risk management, while unable to completely solve the issue of risk, can provide a measure of mitigation.

CYBERSECURITY POLICY, STANDARDS, AND CHECKLISTS

While not as thoroughly studied as purely technical controls [39], it has been argued that one of the most important cybersecurity controls that can be introduced into an organization is the cybersecurity policy [69] [70] [71] [72] [73]. Studies have suggested that most cybersecurity decisions within small to medium-sized organizations are directly guided by cybersecurity policy [74] while large organizations institutionalize cybersecurity in their culture through the use of cybersecurity policy [75]. The term "policy" itself has been argued, with Baskerville and Siponen (2002) dividing research into two schools of thought: technical/computer security and non-technical/management security. Technical security policy generally refers to the automated implementation of management policies [76] [77]. This is confused by the term "policy" being used in technical contexts, such as group policies in a directory environment, or access control policies on a firewall. Management policy, as defined within Baskerville and Siponen (2002), is a high-level plan embracing the organization's general security goals and acceptable procedures. Within this perspective, there has been significant study conducted as to the role of cybersecurity policy within the organization.

One area of cybersecurity policy research has worked to inform the development of effective cybersecurity policies, to include the determination of proper scope and breadth [73] as well as key internal and external influences during development [78]. Baskerville and Siponen (2002) suggested a "meta-policy" or policy for the development of policy, as the best method for developing effective cybersecurity policies tailored to an organizational perspective.

Another area of cybersecurity policy research has focused on the human interaction with cybersecurity policy, from the senior management [70] [79] [80] [81] [36] to the end user [82] [72] [83]. D'Arcy and Hovav (2007) suggested that the human interaction has the potential to completely invalidate the effectiveness of security policies, but also that proper implementation of policies within an organization has the potential to reduce misuse [147].

Finally, it has been argued that for the cybersecurity program to be successful, cybersecurity policy must be aligned closely with the needs of the organization. Researchers

have found that organizations have unique needs that must be considered [71] [84] and that a one-size-fits-all perspective is not ideal; further, inflexibility in cybersecurity policy can encourage "developmental duality" or an imbalance between cybersecurity and usability [85]. Research has shown that policies must be as flexible to the changing needs of the organization, as the changes are fluid, facilitating rather than inhibiting organizational emergence [75].

Another segment of cybersecurity research has focused on the development of standards-based security, such as the Generally Accepted Systems Security Principles (1999) and the ISO/IEC 27000 series. These frameworks purport to best secure anything from an individual asset to an entire organization through implementation of a set of controls, usually covering people, processes, and technology.

Understanding how to create value—investing the optimal amount in protecting assets and creating balance—is key.

Cybersecurity evolved with a reliance on checklists and other "one-size-fits-all" measures aimed at finding the specific minimum control set that will best protect information systems in general [86]. These measures have evolved primarily from the government sector, which has attempted to achieve cybersecurity success through the use of regulated certification and accreditation requirements. The U.S. government, for example, has developed a series of control frameworks (e.g., Department of Defense Information Technology Security Certification and Accreditation Program (DITSCAP), Department of Defense Information Assurance Certification and Accreditation Program (DIACAP), Risk Management Framework (RMF)) that mandate sets of controls across the board based on the integrity, availability, and sensitivity requirements of the IS. These required controls often involve lengthy risk assessments and documentation creation along with stringent technical controls, attempting to secure the people, processes, and technology that power the IS. Internal or third-party certification exercises are often required to validate the implementation. After successful accreditation is received, regular reporting requirements are the norm. Finally, the process is often required on a recurring basis dependent on the sensitivity of the IS.

Closely related to certification and accreditation frameworks are IS governance and management frameworks. While the context [35] [87] [88] differs from governmental control structures, they are very similar in their stated goals: cybersecurity frameworks attempt to ensure the CIA of business information coming into contact with the people, processes, and technology that comprise everyday business operations [89] through the use of mandated controls. Cybersecurity governance and management frameworks have evolved from IT

governance and management frameworks, such as the Control Objective for Information and Related Technology (COBIT) and the Information Technology Infrastructure Library (ITIL). These frameworks have a very limited focus on cybersecurity, with a small number of controls considered alongside other areas like service desks. Purely cybersecurity frameworks, such as the ISO/IEC 27001 (formerly the BS 7799/ISO 17799), have included the Plan/Do/Check/Act cycle that evolved from IT governance frameworks, implementing cycles to establish controls, implement controls, assess controls, and refine based on the results of assessment. These standards have developed within industry, but academia has begun development of frameworks that attempt to apply cutting-edge theories for industry practice. An example is the von Solms and von Solms (2006) Direct-Control Model, and the Business Model for Information Security, developed through the University of Southern California (ISACA, 2009) and licensed through the Information Systems Audit and Control Association.

Finally, cybersecurity maturity criteria have been a burgeoning topic of research. Maturity criteria aim to offer an objective scale for classifying an organization's cybersecurity posture, from low to high. These criteria not only offer a "goal" for improvement but also can be viewed as differentiating an organization from its competitors based on a quantified assessment of successful cybersecurity control implementation. The System Security Engineering Capability Maturity Model, a product of research done at Carnegie Mellon University has received the most attention [90], but alternate models do exist.

ECONOMICS OF CYBERSECURITY

As information as an asset increases in importance, many researchers [93] [94] [95] have discussed the organizational value of information systems and how their protection supports and furthers the business as a whole. Since most measures—technical, personnel, procedural—involve some level of resource allocation, spending on cybersecurity has become an important priority within organizations [94]. Understanding how to create value—investing the optimal amount in protecting assets and creating balance—is key. A good deal of research has focused on deriving the optimal amount for an organization to invest in securing their IS and related assets [96] [97] [98] [99] [100] [101] [102] [93] [103] [94] [95]. This research stream has culminated in the development of models for predicting this optimal amount of cybersecurity investment e.g., [94] [104] [105]. Finally, as large amounts of money are allotted for cybersecurity measures, stakeholders have begun to demand results that they can see, to justify these expenditures. Traditional economic ideas, such as Return on Investment (ROI), have been discussed, with researchers attempting to determine if tools such as Return on Security Investment (RoSI) [94] and the Analytic Hierarchy Process (AHP) [105] would be useful for explaining cybersecurity investments.

A further factor that has been considered is the true cost of IS insecurity; it has been found that there is a highly significant negative market reaction to cybersecurity breaches,

especially when involving unauthorized access to confidential data [107]. This fact is further compounded for certain market segments, such as Internet-specific firms and software vendors, who are subjected to even greater risk of losses due to security breaches [108] [109]. Further, research has shown that even unpublished breaches can have a devastating economic effect on a firm [111]; organizations cannot hide from their vulnerabilities and expect to come out unscathed. Incentives are not only monetary, however; multiple studies have discussed the incentives created by regulations like the Sarbanes-Oxley Act [111] [104]. Within these guidelines, there are often economic penalties for non-compliance. This is another economic factor that must be considered when quantifying the cost of cybersecurity.

It is important for stakeholders to stress the value that cybersecurity can create within an organization; however, when attempting to explain how a cybersecurity program creates value for an organization, one cannot focus solely on economic aspects. Research has discussed at length the socio-organizational considerations involved with cybersecurity, such as effects on organizational culture, and their value to the organization [112] [113] [114] [115].

To shed new light on internal threats using fresh perspectives criminological theories have been introduced to the IS domain.

THE USER

Research has suggested that cybersecurity has an almost "self-canceling" phenomenon to consider: the user [116]. Lack of user compliance has been directly tied to a decrease in cybersecurity effectiveness [77]. Since the effectiveness of controls that are put in place to protect information assets are constrained by behaviors of human agents who access, use, administer, and maintain them [30][118] [119], it is clear that the user and their effect on cybersecurity must be considered. Anderson (2001) even argued that information insecurity is as much due to "perverse incentives" as it is to weaknesses in the technical infrastructure.

One line of research deals with counterproductive computer usage and malicious extremes, including insider threats [121] [122] [123] [124] [125] [126] [119] [127] [128]. While firms are shown to spend more resources countering perceived threats originating from external forces [119], it has been argued that the insider threat is perhaps the most significant threat an organization should consider [121] [126] and that the actual number of internally-led breaches suffered cannot be known due to the vast amount of unreported and unknown breaches [127]. Much research centers around General Deterrence Theory-based approaches to solving insider threat [129] [130], theorizing that misuse will decrease as the disincentives increase. Further, studies have shown that increasing internal knowledge of cybersecurity policy and other countermeasures, while not consistent, has the effect

of decreasing misuse from certain internal groups [127]. However, policy alone cannot be relied upon as a deterrent; Siponen, Pahnila, and Mahmood (2010) found social pressures, employee assessments of vulnerability, and the immediacy of threats all play a part in determining employee intention to comply with cybersecurity policy. To shed new light on internal threats using fresh perspectives, criminological theories have been introduced to the IS domain [131].

Another group of research focuses on external threats. These are the threats perhaps most closely identified as hacking [104] or competition [132]. Stanton et al. (2005) found that firms are more concerned with threats originating from external sources; this is perhaps due to the dominance of externally exploited breaches reported in the press [107]. Studies have shown that the perception of external threats—hackers, viruses, and spyware—so dominate cybersecurity programs that even security policy development first considers protection against the external, rather than internal, threat [133]. Research has typically considered the external threat to be fixed and immutable [134], but it has been suggested that external threats do consider the costs and benefits of attack based on information identified through competitor analysis [132].

Another major theme emerging within the cybersecurity domain is the importance of considering the human factor.

A second subset of user research focuses on the awareness of users towards the systems—both the information system and its protective technologies—with which they interact [123] [145]. Research has shown that awareness of technology is central to the formation of user attitudes, and in turn, the user's concern for cybersecurity [136] [137] but is difficult to characterize due to the individual nature of the variable itself [116]. For instance, awareness towards the negative consequences of spyware has been found to motivate users to develop positive attitudes towards protective technologies and their intention to use them [115]. However, research suggests that simply telling users to follow secure practices is not enough; they must be convinced of it [138].

Another research stream attempts to better understand the user's intentions and their effect on cybersecurity. These studies often incorporate theories such as the Theory of Planned Behavior or Theory of Reasoned Action to explain user intention and its effect on subsequent behavior. Research suggests that user intention is affected by a number of external moderators, including organizational commitment [83], codes of ethics [139], cultural factors [140] [115], and social pressures [142]. Further studies have discussed the link between the user's awareness and their intentions towards IS [119] [141] and suggest that user awareness has a direct link to their intentions, which in turn affects behavior. These findings suggest that user intention—ranging from the malicious to the beneficial—might be a key to understanding why users behave in the manner that they do, and the measures that must be taken to prevent or protect against malicious behavior.

MAJOR THEMES OF RESEARCH

The streams of research within cybersecurity differ in their nature, but there are definite themes recurring throughout the domain. Early works within cybersecurity research were significantly technical, and highly prescriptive, with a heavy dependence on checklists and methodological-based approaches aimed at producing a "one-size-fits-all" method of protection. This mindset, while long deemed inadequate by researchers [75] does continue to persist through some governance and standards-based measures currently in use. However, the field as a whole is evolving with the times; researchers have begun to expand into organizational optimization, considering the concepts of balance and emergence. These concepts weave through a considerable number of studies across the cybersecurity domain. An example is the economic research of Gordon and Loeb (2002, 2006), promoting the idea of a balanced cybersecurity program as value maximization by optimal investment into the protection of assets, a highly context-dependent concept. These concepts align with Anderson's (2003) definition of cybersecurity as risks and controls being in balance.

Another major theme emerging within the cybersecurity domain is the importance of considering the human factor present within the IS. While the IS is not solely technical in nature, early research streams within the cybersecurity domain focused primarily on achieving CIA and its fellow tenets through technical methods. A paradigm shift in the domain occurred when the human aspect began to be considered. Da Veiga and Eloff (2007) described cybersecurity as having distinct phases of evolution: the first phase, purely technical in nature, heavily depended on the technological means of securing the IS. The second phase began when the realization was made that the human element urgently needed to be addressed. This realization has been reflected within the body of research; the cybersecurity domain has moved from purely technical considerations to the inclusion of a great number of studies focusing on socio-organizational areas such as culture [140] [115], user awareness [123] [145], and user behavior [119] [141] [142]. Clearly, as research has suggested a powerful mitigating effect presented by the human factor [117] [116], it can be expected that the human factor will continue to be an important consideration across the cybersecurity domain.

Table 1 presents an analysis of cybersecurity constructs regarding Shannon and Weaver's (1949) levels of communication, adapted from Dunkerley and Tejay, 2009 and 2011 [143] [144]. Understanding these factors presented within the structure provided by Shannon and Weaver (1949), the benefits provided through the dynamic relationship between the Technical Level factors (Information Integrity, Information Systems Assurance, and Operations Enablement) and the Semantic Level factors (User Intention and User Knowledge) lead to the Effectiveness Level proffered upon the organization, Cybersecurity Success as adapted from Dunkerley and Tejay (2012) [146].

Communication Levels	Definition	Cybersecurity Dimensions	Seminal Literature
Technical	The accuracy and efficiency of the system producing information.	Information Integrity, Information Systems Assurance, Operations Enablement	Anderson (1972), Wiseman (1986), Denning (1987), Muralidhar et al. (1995), Sandhu et al. (1996), Daniels & Spafford (1999).
Semantic	The success the information has in conveying the intended meaning from sender to receiver.	User Intention, User Knowledge	Dhillon (2001), Siponen (2001), Trompeters & Eloff (2001), Schultz (2002), Vroom & von Solms (2004), Stanton et al. (2005), Dinev et al. (2008).
Effectiveness	Effect of information on the user's behavior.	Cybersecurity Success	Anderson (2001), Gordon and Loeb (2002), Campbell et al. (2003), Hovav and D'Arcy (2003), Tanaka et al. (2005), Arora et al. (2006).

Table 1. Cybersecurity Dimensions for Shannon and Weaver (1949) Communication Levels

CONCLUSION

In an examination of the different aspects of cybersecurity literature, several points are notable. First, an emphasis has been placed on "a means to an end." Research studies have largely focused on measures to address one or more of the technical aspects of cybersecurity, such as an individual aspect of the CIA triad. While this research contributes to the greater understanding of what constitutes that quality of cybersecurity, it is a mistake to believe that only focusing on the technical assets of an organization while failing to consider other dimensions will facilitate a secure organization. Cybersecurity must be viewed as a holistic process rather than a single "fix."

Another issue is with the overwhelming emphasis on individual dimensions as shown within Table 1, without understanding the interactions of those dimensions. A proposed model of cybersecurity success should show a causal process with an intervening factor presented by the user. It is clear that more study should be focused on the entire life cycle of cybersecurity and the interaction between the individual dimensions.

NOTES

1. Center for Strategic and International Studies (CSIS). (2009). *Significant cyber events since 2006.* Retrieved 22 December 2009 from http://csis.org/files/publication/091109_cyber_events_since_2006.pdf.

2. Pisello, T. (2004, October). Is there a business case for IT security? *Security Management.* Retrieved October 18, 2010 from http://www.securitymanagement.com/article/there-business-case-it-security.

3. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

4. Center for Strategic and International Studies (CSIS). (2008). *Securing cyberspace for the 44th presidency.* Retrieved 22 December 2009 from http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf.

5. Gaudin, S. (2007, April 11). Security breaches cost $90 to $305 per lost record. Information Week. Retrieved October 18, 2010 from http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222.

6. Liebenau, J., & Backhouse, J. (1990). *Understanding Information: An Introduction.* London: Macmillan.

7. Tejay, G., Dhillon, G., & Chin, A.G. (2005). Data quality dimensions for information systems security: A theoretical exposition. In P. Dowland, S. Furnell, B. Thuraisingham, & X. S. Wang (Eds.), *Security Management, Integrity, and Internal Control in Information Systems* (pp. 21-39). New York: Springer.

8. Alavi, M., & Leidner, D.E. (2001). Knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly, 25*(1), 107-136.

9. Kane, G.C. (2006). Casting the net: A multimodal network perspective on knowledge sharing. *Dissertation Abstracts International, 67*(09), (UMI No: 1232407861).

10. Lovata, L.M. (1987). Behavioral theories relating to the design of information systems. *MIS Quarterly, 11*(2), 147-149.

11. O'Donovan, B., & Roode, D. (2002). A framework for understanding the emerging discipline of information systems. *Information Technology & People, 15*(1), 26-41.

12. Shannon, C.E., & Weaver, W. (1949). *The Mathematical Theory of Communication.* Urbana, IL: University of Illinois Press.

13. Dhillon, G., & Backhouse, J. (1994). Responsibility analysis: A basis for understanding complex managerial situations. In *Proceedings of the International System Dynamics Conference,* 70-79.

14. Anderson, J.M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308.

15. Dunkerley, K., Tejay, G. (2012). The development of a model for information systems security success. In Measuring Organizational Information Systems Success: New Technologies and Practices, IGI Global.

16. Chang, S.E., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

17. Kaliski, B. (1993). A survey of encryption standards. *IEEE Microcomputers, 13,* 74-81.

18. Blythe, S.E. (2008). Croatia's computer laws: Promotion of growth in e-commerce via greater cyber-security. *European Journal of Law and Economics, 26,* 75-103.

19. Rivest, R. L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

20. Tompkins, T., & Handley, D. (2003). Giving e-mail back to the users: Using digital signatures to solve the spam problem, *FirstMonday, 8*(9).

21. Walsh, M.E. (1981). Software security. *Journal of Systems Management, 32*(10), 6-14.

22. Shimeall, T.J., & McDermott, J.J. (1999). Software security in an internet world: An executive summary. *IEEE Software, 16*(4), 58-62.

23. August, T., & Tunca, T.I. (2006). Network software security and user incentives. *Management Science, 52*(11) 1703-1721.

24. Denning, D. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering. 13*(2), 222–226.

25. Daniels, T. E., & Spafford, E. H. (1999). Identification of host audit data to detect attacks on low-level IP. *Journal of Computing Security, 7*(1), 3–35.

26. Vigna, G., & Kemmeerer, R. A. (1999). NetSTAT: A network-based intrusion detection system. *Journal of Computing Security, 7*(1), 37–71.

27. Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information Systems Security, 3*(3), 186–205.

28. Frincke, D. (2000). Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information Systems Security, 3*(1), 1–29.

29. Krauss, M., & Tipton, H. (2002). *Handbook of Information Security Management.* Boca Raton, FL: CRC Press.

30. Ma, Q., Johnston, A.C., & Pearson, J.M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

31. Hayam, A., & Oz, E. (1993). Integrating data security into the systems development life. *Journal of Systems Management, 44*(8), 16-21.

32. Leiwo, J., Gamage, C., & Zheng, Y. (1999). Organizational modeling for efficient specification of information security requirements. In *Proceedings of the Advances in Databases and Information Systems: 3rd East European Conference (ABDIS),* 247-260.

33. Byrnes, F., & Proctor, P. (2002). *The Secured Enterprise: Protecting Your Information Assets.* Upper Saddle River, NJ: Prentice Hall.

34. Rosenthal, D. (2002). Intrusion detection technology: Leveraging the organization's security posture. *Information Systems Management, 19*(1), 35-44.

35. Moulton, R., & Coles, R.S. (2003). Applying information security governance. *Computers & Security, 22*(7), 580-584.

36. von Solms, S.H. (2005). Information security governance–Compliance management vs operational management. *Computers & Security, 24,* 443-447.

37. McFadzean, E., Ezingeard, J., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. *Journal of Information System Security, 2*(3), 3-48.

38. Kotulic, A.G., & Clark, J.G. (2004). Why there aren't more information security research studies. *Information & Management, 41,* 597-607.

39. Straub, D.W., & Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

40. Sun, L., Srivastava, R.P., & Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems, 22*(4), 109-142.

41. Perschke, G.A., Karabin, S.J., & Brock, T.L. (1986). Four steps to information security. *Journal of Accountancy, 161*(4), 104-113.

42. Guarro, S.B. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers and Security, 6*(6), 493-504.

43. Pickard, R. (1989). Computer crime. *Information Center, 5*(9), 18-27.

44. Rainer, R.K., Snyder, C.A., & Carr, H.H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129-147.

45. Post. G.V., & Diltz. J.D. (1986). A stochastic dominance approach to risk analysis of computer systems. *MIS Quarterly, 10*(4), 363-375.

46. Woody, C. (2006). *Applying OCTAVE: Practitioners report.* Carnegie Mellon University.

47. Misra, S.C., Kumar, V., & Kumar, U. (2007). A strategic modeling technique for information security risk assessment. *Information Management & Computer Security, 15*(1), 64-77.

48. Cheswick, W.R., & Bellovin, S.M. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Reading, MA: Addison-Wesley Publishing Company.

49. Russell, D., & Gangemi, G.T. (1991). *Computer Security Basics.* Sebastopol, CA: O'Reilly.

50. Cohen, F.B. (1995). *Protection and Security on the Information Superhighway.* New York: John Wiley.

51. Neumann, P., & Parker, D. (1989). A summary of computer misuse techniques. In *Proceedings of the 12th National Computer Security Conference.*

52. Amoroso, E.G. (1994). Fundamentals of Computer Security Technology. Saddle River, NJ: Prentice-Hall PTR.

53. Perry, T., & Wallich, P. (1984). Can computer crime be stopped? *IEEE Spectrum, 21*(5).

54. Landwehr, C.E., Bull, A.R., McDermott, J.P., & Choi, W.S. (1994). A taxonomy of computer security flaws. *ACM Computing Surveys, 26*(3), 211-254.

55. Stallings, W. (1995). *Network and Internetwork Security Principles and Practice.* Englewood Cliffs, NJ: Prentice Hall.

56. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

57. Kokolakis, S. A., Demopoulos, A. J. & Kiountouzis, E. A. (2000). The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security, 8*(3), 107-116.

58. Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.

59. Alter, S., & Sherer, S.(2004). A general, but readily adaptable model of information system risk. *Communications of the AIS, 14*(1), 1-28.

60. Clements, D. P. (1977). Fuzzy Ratings for Computer Security Evaluation. PhD Dissertation, University of California, Berkeley.

61. Beck, U. (1992). *Risk Society.* London: Sage.

62. Hitchings, J. (1996). A Practical Solution to the Complex Human Issues of Information Security Design. In I*nformation Systems Security: Facing the Information Society of the 21st Century.* London: Chapman & Hall.

63. McGaughey, R.E., Snyder, C.A., & Carr, H.H. (1994). Implementing information technology for competitive advantage: Risk management issues. *Information & Management, 26*(5), 273–280.

64. Webler, T., Rakel, H., & Ross, R. J. S. (1992). A Critical Theoretical Look at Technical Risk Analysis. *Industrial Crisis Quarterly, 6,* 23-38.

65. Jarvenpaa, S.L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly, 15*(2), 205–227.

66. Coles, R.S., & Moulton R. (2003). Operationalizing IT risk management. *Computers and Security, 22*(6), 487-493.

67. Rycroft, S., & Tully, M. (2007). Building an information security meta standard. *BT Technology Journal, 25*(1), 37-40.

68. Bodin, L.D., Gordon, L.A., & Loeb, M.P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64-68.

69. Parker, D.B. (1998). *Fighting Computer Crime– A New Framework for Protecting Information.* New York: John Wiley & Sons.

70. Perry, W.E. (1985), *Management Strategies for Computer Security.* Boston, MA: Butterworth-Heinemann.

71. Schweitzer, J.A. (1982). *Managing Information Security: A Program for the Electronic Information Age.* Boston, MA: Butterworth-Heinemann.

72. Warman, A.R. (1992), Organizational computer security policy: The reality. *European Journal of Information Systems, 1*(5), 305-310.

73. Hone, K., & Eloff, J.H.P. (2002). Information security policy–What do international information security standards say? *Computers & Security, 21*(5), 402-409.

74. Briney, A., & Prince, F. (2002). Does size matter? Accessed from www.infosecuritymag.com/2002/sep/2002survey.pdf.

75. Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

76. Sterne, D.F. (1991). On the buzzword 'security policy'. *In Proceedings of the IEEE Computer.*

77. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

78. Tanenbaum, A. (1992). *Modern Operating Systems.* Englewood Cliffs, NJ: Prentice-Hall.

79. Knapp, K.J., Morris, R.F., Marshall, T.E., & Byrd, T.A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508.

80. Gondek, C. (1989). Establishing information security. *Management Accounting, 70*(10), 34-37.

81. Kwok, L., & Longley, D. (1997), Code of practice: A standard for information security management. In *Proceedings of the IFIP TC11 13th International Conference on Information Security.*

82. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

83. Belden, M. (1989). The employee's role in protecting information assets. *Computers & Security, 8*(6), 487-493.

84. Herath, T., & Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-126.

85. Wood, C.C. (1999). *Information Security Policies Made Easy.* San Rafael, CA: Baseline Software.

86. Baskerville, R. (1992). The developmental duality of information systems security. *Journal of Management Systems, 4*(1), 1-12.

87. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375-413.

88. Poore, R. (2006). Information Security Governance. In Handbook of *Information Security Management.* Boca Raton, FL: CRC Press.

89. Da Veiga, A., & Eloff, J.H.P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

90. Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23,* 638-646.

91. Siponen, M.T. (2005). Analysis of modern IS security development approaches: Toward the next generation of social and adaptable ISS methods. Information and Organization, 15, 339-375.

94. Anderson, R. (2001). Why Information Security is Hard—An Economic Perspective. In Proceedings of 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, 10-14.

95. Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

96. Gordon, L.A., & Loeb, M.P. (2006). Budgeting process for information security expenditures. Association for Computing Machinery. *Communications of the ACM, 49*(1), 121-125.

97. Millen, J. (1992). A resource allocation model for denial of service. In *Proceedings of the 1992 IEEE Symposium on Security and Privacy.* Los Alamitos, CA: IEEE Computer Society Press.

98. Luotonen, O. (1993). *Risk management and insurances.* Painatuskeskus Oy, Helsinki, Finland.

99. McKnight, L., Solomon, R., Reagle, J., Carver, D., Johnson, C., Gerovac, B., Gingold, D. (1997). Information Security of Internet Commerce. In *Internet Economics.* Cambridge, MA: MIT Press.

100. Finne, T. (1998). A conceptual framework for information security management. *Computers & Security, 17*(4), 303–307.

101. Jones, M.R. (1997). It all depends what you mean by discipline. In Mingers, J., & Stowell, F. (Eds.), *IS: An Emerging Discipline?* London: McGraw-Hill.

102. Buzzard, K. (1999). Computer security-What should you spend your money on. *Computers & Security, 18*(4), 322–334.

103. Hoo, K. (2000). How much is enough? A risk-management approach to computer security. A Consortium for Research on Information Security Policy (CRISP) Working Paper. Stanford, CA: Stanford University.

104. Meadows, C. (2001). A cost-based framework for analysis of denial of service in networks. *Journal of Computer Security, 9*(1/2), 143–164.

105. Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25,* 629-665.

106. Huang, C.D., Hu, Q., & Behara, R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics, 114(2) 793-804.

107. Bodin, L., Gordon, L.A., & Loeb, M.P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78-83.

108. Campbell, K., Gordon, L.A., Loeb, M.P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security,* 431-448.

109. Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

110. Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering, 33*(8), 544.

111. Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers, 8*(5), 350-362.

112. Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Sohail, T. (2006). The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. *Journal of Accounting and Public Policy, 25*(5), 503-530.

113. Backhouse, J., Hsu, C.W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly, 30,* 413-438.

114. Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16,* 293-314.

115. Drevin, L., Kruger, H.A., & Stegn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26,* 36-43.

116. Dinev, T., Goo, J., Hu, Q., & Nam, K. (2008). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

117. Dodge, R.C., Carver, C., & Ferguson, A.J. (2007). Phishing for user security awareness. *Computers & Security, 26,* 73-80.

118. Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

119. Stanton, J.M., Stam, K.R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security, 24,* 124-133.

121. Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171–175.

122. Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20,* 165-172.

123. Siponen, M.T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal, 14*(4), 15-23.

124. Trompeters, C.M., & Eloff, J.H.P. (2001). A framework for the implementation of socio-ethical controls in information security. *Computers & Security, 20,* 384-91.

125. Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*(6), 526-531.

126. Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91–95.

127. D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89,* 59-71.

128. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105.

129. Tittle, C. R. (1980). *Sanctions and Social Deviance: The Question of Deterrence.* NY: Praeger.

130. Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

131. Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems, 15,* 403-414.

132. Gordon, L.A., & Loeb, M.P. (2001). Using information security as a response to competitor analysis systems. Communications of the ACM, 44(9), 70-75.

133. Smith, H.J. (1994), *Managing Privacy: Information Technology and Corporate America.* Chapel Hill, NC: University of North Carolina Press.

134. Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26,* 639-688.

136. Goodhue, D.L., & Straub, D.W. (1991). Security concerns of system users: A study of perception of the adequacy of security measures. *Information and Management, 20*(1), 13–27.

137. Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

138. Pfleeger, C.P., & Pfleeger, S.L. (2003). *Security in computing* (3rd ed.). Prentice Hall.

139. Harrington, S.J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

140. von Solms, B. (2000). Information security – The third wave? *Computers & Security, 19*(7), 615-620.

141. Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

142. Siponen, M., Pahnila, S., & Mahmood, M.A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

143. Dunkerley, K., Tejay, G. (2009). Developing an information systems security success model for e-government context. In Proceedings of the 2009 Americas Conference on Information Systems, San Francisco, CA.

144. Dunkerley, K., Tejay, G. (2011). A confirmatory analysis of information systems security success factors. Hawaii International Conference on System Sciences.

145. Thomson, M.E., von Solms. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167.

146. Dunkerley, K., Tejay, G. (2012). The development of a model for information systems security success. In Measuring Organizational Information Systems Success: New Technologies and Practices, IGI Global.

147. D'Arcy, J., & Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information Systems Security, 3*(2), 3-30.

Direct Commission for Cyberspace Specialties

Colonel Andrew O. Hall
Major Brian M. Schultz

ABSTRACT

The US Army executes small-scale direct commission programs for specialties needed within the profession of arms. When expanded into Cyberspace, similar programs can provide an opportunity to enhance readiness and capability while building toward a force of the future. A Cyberspace direct commission program can serve as a test case for removing the traditional bar to lateral entry for technical specialties. Challenges relating to culture, development, and operations may arise during implementation of such a program. This paper hopes to start the initial discussion on these topics and introduce ideas about future research that can contribute to the Army's assessment of a direct commission program.

INTRODUCTION

During World War II, the Allies adopted a new approach to operational decision making by creating Operations Analysis. During that period, America and its allies felt an exceptional call to service, and 12% of Americans served in the military. [1] The Army employed expert "civilians in uniform" that provided insight to operational questions and weapons performance using mathematical and statistical techniques. [2] This new approach to operational decision making produced a new discipline. During later conflicts like Vietnam, the Army grew the analytical community to tackle new challenges. [3] The Operation Research/System Analysis functional area exists to this day; although, current officers only transfer into the discipline from other branches within Army.

On the last day of 2016, the Department of Defense's (DoD) active duty military and civilian workforce totaled 2,052,573. [4] On the same day, the Census Bureau estimated the population of the United States to be 324,304,407, [5] meaning that 0.6% of Americans served the military in either a uniformed or civilian capacity. Currently, a limited number of Americans answer the call to military service; however, the Nation increasingly

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

faces a number of threats in Cyberspace. While the Army has actively responded to this changing landscape by standing up units, occupational specialties, educational programs, and the Cyber branch itself, now is the best time to explore all options.

A direct commission program for civilian experts in the Cyberspace domain provides an additional opportunity to enhance readiness and capability while building toward a force of the future. Just as the conflict of World War II drove the need to employ "civilians in uniform" and develop Operations Analysis as a discipline, challenges in the Cyberspace domain may require the Army to draw on civilian experts to solve technological problems. Throughout the Nation, an ecosystem already exists, traversing academia and industry, that creates expert professionals through a combination of classroom and on-the-job experiences. A direct commission program can leverage this unique American resource. Waiting to establish such a program until a time of national crisis lacks foresight. Previous direct commission programs for technical experts were enacted during a time of national service through the military draft. A new process should be entertained for our all-volunteer Army.

THE PROFESSION OF ARMS

Individuals entering into military service also enter into the profession of arms. The Center for the Army Profession and Ethic has defined the Army profession as a "unique vocation of experts certified in the design, generation, support, and ethical application of landpower serving under civilian authority and entrusted to defend the Constitution and the rights and interests of the American people."[6] This definition does not limit initial service to junior level positions, and yet the Soldier is traditionally viewed as a profession with a bar to lateral entry, without regard to experience or expertise.

MAJ Brian Schultz is a research scientist at the Army Cyber Institute and teaches computing courses in the Department of Electrical Engineering and Computer Science at the United States Military Academy. From 2014-2015, he served as the Chief of Cybersecurity for the 8th Theater Sustainment Command at Ft. Shafter, HI. He has over ten years of information systems experience and has deployed as a Signal officer in support of Operation Iraqi Freedom. He holds an M.S. in Information Assurance from Norwich University and a B.A. in Communications from Millikin University. He is currently a graduate student studying Computer Science at DePaul University and his research interests include talent management, data science, and machine learning.

As Samuel Huntington argues in The Soldier and the State, mastery of military officership requires professionalism on par with an attorney or doctor.[7] Unlike the professions of law or medicine, a single employer, the DoD, holds a monopoly on the indoctrination into and employment of individuals in the profession of arms. When combined with a bar to lateral entry, this creates a closed personnel system, which requires the need to grow nearly all uniformed technical experts and senior leaders from within the DoD itself.[8] Given the competitive job market surrounding Cyberspace and other IT specialties, this traditional closed system may prove inadequate to sustain the best talent. Now is the time to reconsider this system and potentially remove the bar to lateral entry for a variety of specialties.

A lateral entry exists only in a small subset of the Army, primarily in the medical field. It is accepted that a direct commission applicant specializing in medicine already participates in a profession with standards, self-regulation, and state licensing. Upon entry into the Army, the medical officer does not step away from these artifacts of their professional culture. Instead, the direct commission officer takes on an additional profession, the profession of arms. The Army has accepted that the general skills applied to medicine in civilian hospitals traverse the civil-military divide and provide similar benefit in military hospitals.

Secretary Ashton Carter, the U.S. Secretary of Defense from February 2015 to January 2017,[9] believed that the DoD should broaden opportunities of service for all Americans. While the Army profession normally requires Soldiers to enter at the most junior levels, Secretary Carter suggested a permeable force which would allow for the capture of experiences and patriotism from a variety of Americans at varying stages of their professional

development. He envisioned a force of the future in which lateral entry was possible for professionals in and out of uniform to serve at the junior, mid-career, and senior levels in both the active duty and reserve forces. A direct commission pilot program for specialties in Cyberspace can serve as a test case for Secretary Carter's vision. Outcomes observed and lessons learned might someday contribute to creating direct commission programs in other professional areas as well.

Throughout the Nation, an ecosystem already exists that creates expert professionals through a combination of classroom and on-the-job experiences.

The bedrock of service as an officer consists of taking responsibility for victory and defeat, readiness and unpreparedness, success and failure.[10] The Soldier and the State described the nature of officer work as the "management of violence".[11] Huntington chose to stress the word management for good reason, and the role of an officer includes managing operations and leading enlisted Soldiers. The junior enlisted demographic draws some of the best younger adults the Nation has to offer. These enlisted Soldiers swear an oath to obey the orders of officers appointed over them. But in a reciprocal manner, this places just as much burden on the officer corps, as the professional officer must acknowledge and honor the responsibility to lead those that have pledged to follow while promoting their safety, welfare, and development. This creates a clear distinction between the nature of officer work and that of a hired Army civilian.

This nature of officer work surely varies among the different branches of the Army—making some branches more fertile ground in accepting direct commission officers. Regardless of the branch, key cultural, developmental, and operational challenges might arise during implementation of direct commission programs. Injecting direct commission officers into a workforce where none previously existed will likely change notions of workforce equity, leader development, and standard onboarding processes. Leaders will face new challenges in articulating requirements at the individual expert level. These changes could alter our existing promotion selection process and impact future career climates.

The new policies required to enact a direct commission program, implement a reduced onboarding process, and place new employees in expert work roles will alter how a traditional officer views his or her own place within the branch. As two organizational behavior academics, Douglas Hall and Jeffrey Yip, state, "Organizations are constantly transmitting social information about careers, which are then interpreted by employees. In most instances, organizations send mixed career signals to their employees, and this

has an effect of weakening an organization's career climate and ultimately its culture." [12] The Army needs a functioning Cyber branch with a solid career culture and climate. To ensure success, we hope to begin the discussion on these topics while offering some initial considerations.

WHERE CYBER STANDS

The Cyber community has already acknowledged the idea that acquiring and developing the talent required for Cyberspace operations may come from nontraditional sources or by nontraditional means. This creates a notable difference between technical talent in Cyberspace and the other warfighting domains. The institutions that best develop the skills required for landpower combat lie within the Army's closed personnel system itself; whereas the skills required of a Cybersecurity leader or technician can be developed both in and out of uniform. This idea has already found its way into law, and soon it will take hold in a pilot program for the Army.

The 2017 National Defense Authorization Act included a provision that allowed a pilot program for the direct commission of officers for Cyberspace specialties. [13] The Army took on the responsibility of piloting their direct commission program as of January 30th, 2017. In February, Brigadier General J.P. McGee, Army Cyber Command's Deputy Commander for Operations, acknowledged the continual need to close capability gaps. He stated, "Cyber space threats and challenges are only continuing to increase, and we're continually trying to keep pace with our defensive measures." [14]

> The bedrock of service as an officer consists of taking responsibility for victory and defeat, readiness and unpreparedness, success and failure.

In March 2017, the Army G1 developed an operational planning team to develop the details of this new direct commission pilot program. During this initial planning, the Cyber community will need to take steps to develop requirements within Cyberspace workforce structures. Also, the community will need to develop methods for assessing traditional versus nontraditional talent from various sources. Breaking ground on this pilot program offers a path for initial direct commissions and raises several potential research questions, as discussed in subsequent sections.

OPPORTUNITIES FOR SERVICE

We aim to offer considerations for the direct commission program and to begin the discussion on how this program might impact the employment, retention, and career culture of officers in the Cyber branch. It is important that the Cyber community proceeds with the direct commissioning of officers in a deliberate and well-planned approach.

Direct commission officer candidates must have a consistent and demonstrable expertise, a sense of patriotism, and appropriate skills for the Army. A combination of these attributes should positively impact operations, help the Cyber branch determine its nature of work, and support a positive career climate as seen by branch's junior officers. Creating such a peacetime lateral entry system prepares for potential growth of the Army's Cyber workforce.

By implementing a direct commission program, the Army will look outside the traditional boundaries to allow a broader pool of applicants to fill jobs in the Cyber workforce. It is important to note that an array of opportunities already exist for potential applicants. Current work roles roughly equate to the following civilian-friendly titles: security analyst, exploitation analyst, penetration tester, planner, operations manager, and developer. The table below illustrates how the direct commission program fits into the opportunities already available for those who would like to serve.

Type of Service	Work Role	Work Level	Initial Training in Months	College Requirement	Annual Pay in Maryland Area
Junior Enlisted	Security Analyst, Exploitation Analyst	Entry-Level Worker	12	No College	$53K, after 4 Years of Service
Warrant Officer	Penetration Tester	Skilled Technician	Lateral Entry Not Authorized	Some College	$82K, varies with Time in Service
Entry-Level Officer (Staring at O-1)	Planner, Manager, Developer	Entry-Level Leader	14	Bachelor's Degree	$78K, after 2 Years in Service
Direct Commission (O-3 start assumed)	Planner, Manager, Developer	Leader or Expert	3	Bachelor's Degree	$95K, after 2 Years in Service
Army Civilian	Planner, Manager, Developer	Leader or Expert	Not Significant	Position Dependent	$44K - $131K, Grade Dependent
Highly Qualified Expert	Miscellaneous	Expert	Not Significant	Position Dependent	May not exceed salary of VP

Table 1. Summary of Cyber Workforce: An Array of Opportunities

This table summarizes our earlier work published in *The Cyber Defense Review* online.[15] The pay figures included in the table offer a very rough generalization of expected annual salaries for various types of service and work roles. These figures include allowances for subsistence and housing in the Maryland area. Also of note, junior enlisted Soldiers receive advanced training and gain skills more traditionally acquired from higher education. One could consider the training that these Soldiers receive as a form of compensation itself.

The direct commission program creates an additional option for serving in the Army's Cyber workforce, and the remainder of this paper will focus on this opportunity. As illustrated in the above table, direct commissioning offers a shorter initial training program than that for entry-level officers. This reduced onboarding is possible because a directly commissioned officer would bypass the traditional path for civilians to become an officer. This path normally consists of Basic Combat Training, Officer Candidate School, and the Basic Officer Leader Course and lasts longer than one year in duration.

This lengthy process remains insufficient to commission officers that can quickly begin work on the biggest challenges facing the Cyber workforce. A direct commission program provides the Army the ability to quickly onboard a professional, similar to the process of hiring a civilian. Direct commission officers could start at a pay grade commensurate with their civilian experience, skill, and education level. For this reason, the above table uses an officer in the grade of 0-3 to estimate the direct commission salary figure. While a direct commission program offers similar benefits to a direct civilian hire process, the role of a commission officer is distinct from that of an Army civilian within the profession of arms, as discussed in previous sections.

Direct commission officer candidates must have a consistent and demonstrable expertise, a sense of patriotism, and appropriate skills for the Army.

The DoD has another recent example of injecting talent into its technical workforce. The Defense Digital Service (DDS) has seen success through an effort to direct hire civilians to team with military members to tackle tough problems relating to defense technologies, information sharing, and collaboration.[16] Upon creating DDS in 2015, Secretary Carter conveyed the usefulness of bringing unique talents from outside the department's bureaucracy to harness agile approaches to complex problems. He stated that we could benefit from innovative entrepreneurs "who will work with senior leaders on some of our most challenging projects for two years at a time."[17]

Like DDS, the creation of a direct commission program does not declare that current Cyber officers lack expertise in the Cyberspace domain; rather, the program simply allows

for the injection of new life blood and diversity of thought into the Cyber branch, similar to a "training with industry" program in reverse. As a result, an exchange of talent across civilian-military lines should promote the practice of striving for new and unique ways to solve challenging problems throughout the entire branch. In addition, the Cyber branch might also consider more permeable forms of employment that would allow for easier transitions from reserve to active service, if the talent sought by the active component can be filled by a member of the Reserve Component or National Guard workforce.

During the creation and execution of a direct commission program, the Army must consider challenges pertaining to onboarding practices and career culture artifacts. In the following sections, we highlight some of these aspects to such a program.

CURRENT DIRECT COMMISSION PRACTICES

In specialty branches, the Army has existing practices in which professionals directly commission as officers. These fields include the Medical Corps, Judge Advocate General's Corps, and Army Chaplains. Two distinctions are important to note regarding these specialty areas and the Cyber branch. First, these specialty branches do not deliver combat effects to adversaries. These officers serve in support roles; however, the Cyber community may need its direct commission officers to deliver combat effects against adversaries. This drives a need for these officers to understand the law of war and a general sense of military operations. Secondly, direct commission officers in the specialty branches mentioned above normally obtain a state-granted license to practice their profession. Thus, the official vetting of job skills is performed through a third party. Conversely, state licenses to practice software development, penetration testing, or other Cybersecurity work roles are either non-existent or rarely required in the commercial job market. Therefore, the Cyber community must determine a way to evaluate the skill level of direct commission officers.

Coincidently, the Army has another specialty area in which it recruits direct commission officer candidates from a profession that has no state licensing—namely the Army band program. In order to direct commission into the Army band program, a candidate must audition. The act of auditioning establishes a process in which the candidate must execute an observable skill. The Cyber community should develop a similar audition or assessment process to observe and evaluate the demonstrable skills of candidates seeking technical positions. The Cyber community could first consider eligible candidates based on a combination of education, experience, and certification, all signals of quality, but should then observe candidates through a hands-on assessment.

Officers in Army specialty branches typically experience a reduced onboarding process. New Army doctors and nurses attend the Basic Officer Leader Course at Fort Sam Houston. This program ranges from ten to fourteen weeks in duration, depending on medical specialty and prior military service experience.[18] New Army attorneys complete

the Direct Commission Officer Course at Fort Benning and a ten-week familiarization with the Judge Advocate General's Corps.[19] Army band officers also attend an officer basic course.[20]

These specialty branches reduce the onboarding time for new officers because their direct commission programs have already determined that the officer meets the technical criteria for the position. These onboarding courses serve as familiarization with the Army and an induction into the profession of arms. While attorneys, doctors, and chaplains have already established professional identities with skills that traverse the civilian-military divide, an onboarding process is always necessary to properly introduce these professionals to their new additional profession, the profession of arms.

In a rush to direct commission officers with unique talents, the Cyber branch must not shortchange the onboarding process for professionals with Cyberspace specialties. The Cyber branch must develop an onboarding program that introduces new officers to the profession of arms. The existing Direct Commission Officer Course at Fort Benning combined with a Cyber planner or Cyber operations course at Fort Gordon would satisfy this need. If planned for efficient execution, this onboarding program could last twelve weeks. In light of this notion, the next section discusses aspects of military requirements that the Army expects of all officers in the profession of arms.

The Cyber branch might consider more permeable forms of employment that would allow for easier transitions from reserve to active service.

ARTICULATING THE REQUIREMENT

In branches other than these specialty areas, the Army has two methods of obtaining skillsets: (1) developing recruits or existing Soldiers to required levels, or (2) writing position descriptions and hiring Army civilians. Direct commissioning an officer creates a unique third method. Before the Army considers a position for direct commission, questions should be answered regarding the two methods listed, namely: (1) can the Army develop an existing Soldier promptly, or (2) could a civilian hire fill the gap?

The first method of developing an existing Soldier is essentially internal talent reallocation. This method often occurs in the Army. The Special Forces branch and the many Army functional areas have defined needs through which the requirement for talent is then understood. Against these talent requirements, the Special Forces branch and the functional areas can develop accurate assessments to narrow down the pool of possible applicants. In the case of the Special Forces branch, the Special Forces Assessment and Selection (SFAS) program forms the basis for this step in the broader talent reallocation process. While

Cyberspace specialties will require new and unique skillsets in a completely different domain, the foundational need to articulate the requirement must precede the development of the selection process itself.

Internal talent reallocation also requires the Army, a traditionally closed system, to develop expertise in-house, a method not popular in industry's talent marketplace. This aspect of talent management endured by the military, makes a direct commission program appear beneficial for niche technical skills. Developing these skillsets through a talent reallocation process might require significant resources. Direct commissioning an officer minimizes this burden, but unlike a civilian hire, creates a Soldier and leader in the profession of arms.

The Army created the Cyber branch to grow maneuver officers in Cyberspace. Cyber officers are expected to direct and lead operations. A direct commission officer may or may not lead a team or command a battalion; however, the direct commission program should not necessarily preclude an officer from leadership if they prove to be the best candidate for the position. To deny the most qualified individual a leadership position based on the officer's commissioning source only reinforces military's closed personnel system and traditional biases regarding leadership that may not hold true in the future.

The Cyber community can begin to look to industry and other free markets of employment to understand best practices and draw insight from existing empirical data.

Even if a direct commission officer never leads a team or commands a battalion, junior officers, warrant officers, and enlisted Soldiers will still view the direct commission officer as an informal leader with subject matter expertise. This aspect of informal leadership will impact the career culture and climate of the branch. Considering this idea, the following paragraphs highlight some of the considerations for professional knowledge, skills, and abilities that should be considered when direct commission officers fill grades on par with direct and organizational leaders.

All Army officers executing direct level leadership have obtained a four-year college degree. The well-rounded education provided at our Nation's universities ensures that an officer has a diverse educational background accompanied by the reading, writing, and presentation skills necessary to provide well-articulated orders and directives and to brief superiors with meaning and coherence. Regarding this sort of knowledge, direct commission officers should have commensurate understanding similar to that of all other officers. Other knowledge requirements of direct commission officers should be

well-thought out but may include the following: understanding the law of war, our system of military justice, operational security, and joint cyber operations. Officers from traditional commissioning sources grasp this knowledge, and the Basic Officer Leadership Course and Captains Career Course reinforce knowledge in these areas for direct level leaders. Direct commission officers should be no less knowledgeable.

In addition to knowledge, articulating the requirement for direct commission officers also means determining the skills and abilities needed to fills shortfalls in capability and capacity. The Cyber community may very well need to further define the nature of officer work in the Cyberspace domain to acutely define these skills and abilities. One idea of note is that direct commission officers themselves will influence how the future nature of officer work in the Cyber branch is defined, creating an interesting lifecycle as depicted in Figure 1.

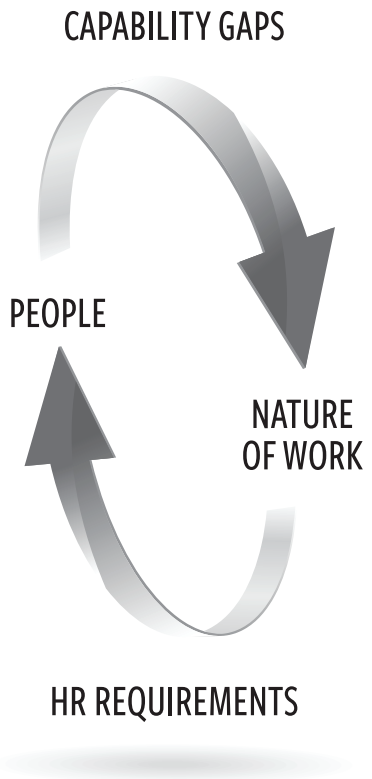


Figure 1. People – Nature of Work Lifecycle

Direct commission officers filling grades on a par with operational level leaders also have knowledge requirements that must be considered. The Army expects operational level leaders to know the doctrinal and theoretical concepts to understand military strategy and to manage and plan for change in complex joint and multinational environments. Operational leaders should also understand organizational climates and leadership in a changing world.[21] Traditional officers gain an education in these topics during the Command and General Staff Officers' Course. The Army War College reinforces and expands on these concepts. Direct commission officers that serve in grades on par with operational level leaders should be no less knowledgeable.

As a challenge to these requirements, the Cyber branch must address the non-selection of expert officers at promotion boards. The Army has already passed over Cyber officers with a high level of education in technical fields. Obtaining post-graduate education in a technical field often requires an officer to spend years outside the operational force, thus translating to fewer evaluation reports. This puts the officer at a disadvantage during promotion boards. While other valid reasons to non-select these officers may exist, their non-promotion sends a social cue to Cyber officers that devalues education, especially a technical education. Combined with a direct commission program aimed to onboard

professional and technical experts, this practice would send a conflicting "mixed signal", as illustrated by Hall and Yip.[22] In order to retain fully qualified individuals, the Cyber branch should conduct further research regarding careers and seek to understand the branch's new place within a Cyber-related job market that extends beyond the lines of the military.

Only through exploring all options to attract the best current and future professionals does the Army maximize its ability to enhance readiness and capability.

FURTHER RESEARCH

Other areas of research may include the impact direct commissions have on aspects of learning versus performance culture, protean and organizational career orientations, and inclusive versus exclusive climates. The Cyber branch should also seek to understand how direct commissions might affect equity in the workplace. Aside from specialty pays, the Army has little difference in pay among officers of the same rank, yet the officer corps functions like a meritocracy. Officers with more perceived skill or value achieve promotions at a higher rate. Further research should consider how an influx of expert talent impacts equity among officers in the branch. In quickly onboarding expert professionals through a direct commission program, the Cyber branch effectively relieves itself of in-depth development for some of its members, relying instead on previously obtained education and job experience. This upsets the talent management paradigm of acquire, develop, employ, and retain. Further research should also be done to understand how this impacts the branch as a whole. For some of this research, the Cyber community can begin to look to industry and other free markets of employment to understand best practices and draw insight from existing empirical data.

A direct commission program may also benefit the future Cyber workforces for the Army Reserve and National Guard. The National Guard has a composition different from the active duty workforce in which Army civilians fill staff authorizations throughout the force structure. The National Guard has no authorizations for civilian positions; hence, the Cyber community must consider how to adjust or translate roles and responsibilities when applied to the National Guard force structure. Just as a path to lateral entry may enable expert professionals to join active duty military service, the Army Reserve and National Guard may additionally benefit from such a program. The Cyber branch should continue to research how a direct commission program might benefit the readiness of the reserve component or National Guard when preparing for responses to crises in the Cyberspace domain.

CONCLUSION

Piloting a direct commission program allows the Cyber branch to create a merit-based system, potentially free of any bias to previous military experience. This promotes Secretary Carter's vision of a permeable form of service capable of allowing skilled and patriotic Americans to serve at any point in life. This program provides another opportunity to leverage the intellectual capacity of the Nation. The Army should also consider that this pilot program can inform future programs for direct commissions in professional areas other than Cyberspace.

As discussed in the previous sections, several aspects related to career culture and the current talent management paradigm could present difficulties for this program at scale. The Cyber community should pursue a small pilot program for this effort and increase the size of the program cautiously as further research is explored. Meanwhile, the Cyber community should continue to promote all options and opportunities for Americans to serve in the Cyber workforce. Only through exploring all options to attract the best current and future professionals does the Army maximize its ability to enhance readiness and capability while building toward the force of the future.

NOTES

1."Americans and Their Military, Drifting Apart," http://www.nytimes.com/2013/05/27/opinion/americans- and-their-military-drifting-apart.html, (accessed February 23, 2017).

2. United States. Department of Defense, Army. *History of Operations Research in the United States Army.* By Charles R. Shrader, Vol. III., Washington, DC: Government Printing Office, 2009, 137-38.

3. United States. Department of Defense. Army. *History of Operations Research in the United States Army.* By Charles R. Shrader, Vol. II., Washington, DC: Government Printing Office, 2008, 156-57.

4. "Armed Forces Strength Figures For December 31, 2016," https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp, (accessed February 23, 2017).

5. "U.S. and World Population Clock," https://www.census.gov/popclock/, (accessed February 23, 2017).

6. United States. Army. Center for the Army Profession and Ethic. The Army Profession Pamphlet, 2012, 2-3.

7. Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations.* Cambridge, MA: The Belknap Press of Harvard University Press, 1957, 12-13.

8. Andrew O. Hall, "Simulating and Optimizing: Military Manpower Modeling and Mountain Range Options." PhD diss., University of Maryland, 2009, 2-4.

9. Ashton B. Carter, http://history.defense.gov/Multimedia/Biographies/Article-View/Article/571296/ashton-b-carter/, (accessed March 10, 2017).

10. Robert J. Dalessandro, *Army Officer's Guide.* 52nd ed. Mechanicsburg, PA: Stackpole Books, 2013, 61-106.

11. Samuel P. Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations.* Cambridge, MA: The B elknap Press of Harvard University Press, 1957, 12-13.

12. Douglas T. Hall and Jeffrey Yip, "Career Cultures and Climates in Organizations." *The Oxford Handbook of Organizational Climate and Culture,* June 2014, 1-2.

13. S. 2943, 114th Cong., Congress.gov (2016) (enacted), 110-111.

14. "Army looking at direct commissions for civilian cybersecurity experts." https://www.stripes.com/news/army-looking-at-direct-commissions-for-civilian-cybersecurity-experts-1.453101, (accessed February 12, 2017).

15. Brian M. Schultz and Andrew O. Hall, "The Cyberspace Workforce: An Array of Opportunities." *Cyber Defense Review.* http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1184498/the-cyberspace-workforce-an-array-of-opportunities/.

16. "Transforming technology within the Department of Defense," https://www.dds.mil/, (accessed February 15, 2017).

17. "Carter Details Force of the Future Initiatives," https://www.defense.gov/News/Article/Article/630400/carter-details-force-of-the-future-initiatives, (accessed March 10, 2017).

18. "Medical Corps Officer (62)," http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/medical-and-emergency/medical-corps-officer.html, (accessed February 17, 2017).

19. "Army Judge Advocate General's Corps Attorney (27A)," http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/legal-and-law-enforcement/jag-corps-attorney.html, (accessed February 17, 2017).

20. "Band Officer Jobs (42C)," http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/arts-and-media/band-officer.html, (accessed February 17, 2017).

21. "Command and General Staff Officers' Course Summary," http://usacac.army.mil/organizations/cace/cgsc/courses, (accessed February 16, 2017).

22. Douglas T. Hall and Jeffrey Yip, "Career Cultures and Climates in Organizations." *The Oxford Handbook of Organizational Climate and Culture,* June 2014, 1-2.

Providing Cyber Situational Awareness on Defense Platform Networks

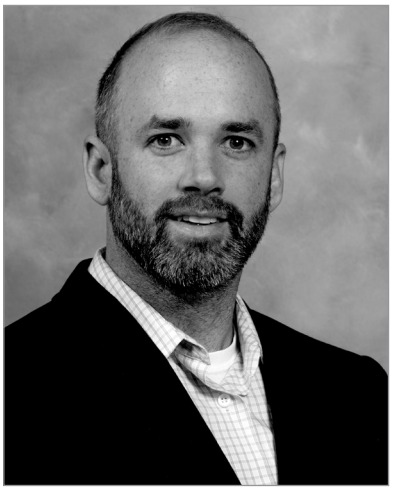
Patrick M. Hayden
David K. Woolrich
Katherine D. Sobolewski

ABSTRACT

Modern defense platforms are at increasing risk of cyber-attack from sophisticated adversaries. These platforms do not currently provide the situational awareness necessary to identify when they are under cyber-attack, nor to detect that a constituent subsystem may be in a compromised state. Long-term improvements can be made to the security posture of these platforms by iterative application of cyber risk assessments and subsystem hardening, but this is a time-consuming and costly task. Monitoring platform communication networks for malicious activity is an attractive solution for achieving improved cyber security on defense platforms in the near term. The MIL-STD-1553 bus is central to the operation of a broad range of defense platforms, making 1553 security solutions generally applicable. This article presents our research into the susceptibility of modern defense platforms to cyber-attack. We discuss risk factors contributing to cyber access, and command and control channels. We then describe a range of platform cyberattack classes, while considering the observables and indicators present on the 1553 bus. Finally, we examine factors and considerations relating to implementation of a "Cyber Warning Receiver" solution approach for detection of such attacks.

THE THREAT IS REAL

For as long as weapons system platforms have been called upon to perform missions in contested spaces, the military has sought to protect the warfighter by equipping these platforms with survivability equipment. This equipment detects threats from across the various domains in which the platform operates, and alerts operators while taking appropriate response measures. As technology and connectivity of these platforms evolves, and increasing sophistication is realized through automation, a new threat domain has emerged. This threat lurks in the dark, escaping detection by human eyes



Patrick M. Hayden is the Chief Engineer for Cyber Electronic Protection programs at BAE Systems. Patrick has 10 years of experience in the cyber security field, performing systems assessment, software reverse engineering, and vulnerability research covering both offensive and defensive perspectives across a wide range of targets and applications.

and ears, yet it has a clear potential for harm to the warfighter and the mission. This is the cyber threat, and it is real.

Cyberattacks become a credible threat if there is a reasonable expectation that a malicious actor could gain access to a defense platform, achieve a persistent malware presence, and subsequently trigger this malware to impart a damaging effect. While there is a lack of openly documented cyberattacks against DoD platforms, published examples against similar systems in other industries provide a compelling case for the feasibility of such attacks.

Unlike traditional kinetic attacks, cyberattacks are not limited in range. In cyberspace, there are no concrete boundaries or borders. A malicious actor in a faraway land can achieve the same reach as someone attacking a target from the same city. Cyberattacks also have greater flexibility in their timing than most traditional attack types. A complete cyberattack may begin well in advance of the realization of any ultimate effect. Attackers can leverage a latent presence at a critical moment in the future to achieve their end goals. This may occur at a predetermined time, or when a predetermined condition is met and may affect a single platform or an entire compromised squadron simultaneously.

Our platforms are at risk regardless of their location, from the battlefield to their home base. Despite these realities, many weapons system platforms operate without sufficient means of providing detailed situational awareness into their cybersecurity state.

LESSONS FROM INDUSTRY

Throughout industry and academia, we hear more and more about attacks against embedded systems and other smart devices. Attacks originate from threats that range from individual troublemakers

David K. Woolrich is a program manager in BAE Systems–Survivability, Targeting, and Sensing Solutions business area. His background is information security, information assurance, and cyber electronic warfare. He is focused on increasing awareness and survivability of DoD assets from cyber attacks.

to state-sponsored hacking groups. These attacks can be foul-mouthed hackers yelling at children via smart baby monitors [1], using SmartTVs as entrance points to home networks [2], entire automobiles being taken over remotely [3], or debilitating modification of industrial control processes [4].

In 2015, security researchers Dr. Charlie Miller and Christ Valasek were able to remotely access an unaltered SUV, controlling everything from the volume of the radio, to the transmission and steering of the Jeep. Initially, takeover of the SUV required access to the USB connection on the automobile, which is normally reserved for vehicle maintenance. With time, however, Dr. Miller and Mr. Valasek were able to gain access to the SUV through its onboard cellular network, traverse multiple Jeep subsystems, and ultimately control physical aspects of the SUV from their hotel room while the Jeep was traveling on a highway.

In 2017, security consultants ARS were able to demonstrate the insertion of malicious code over a broadcasted TV signal. This malicious code was transmitted via the digital video broadcasting—terrestrial signal and once executed allowed full remote control of the TV with no physical access required. The transmitted code was able to exploit a vulnerability in the smart TV's web browser enabling root access for the attacker. If a broadcast station were compromised, this attack could be delivered to any vulnerable TV within the broadcast towers' range.

As systems become more complex and gain more parts, supply chains for devices and systems become more spread out and global. This creates difficultly in validating the pedigree of 100% of the components on any one system. A single system could be comprised of hundreds or thousands of components. Without rigorous vetting of all parts, it is possible that compromised or counterfeit parts could be introduced into the system. This fear was realized by the DoD

Katie D. Sobolewski is a Technology Development Manager for Cyber Electronic Protection at BAE Systems with experience in cyber defense, cyber electronic warfare, and platform protection. Katie has a background in algorithm development, signal processing, and optimization for increased system performance.

when foreign chip manufacturer Lenovo was suspected of introducing phone-home capabilities into their chipsets [5], sparking fear within the US government that their systems could be compromised. A 2017 Defense Science Board Task force on Cyber Supply Chain confirms the supply chain to be a real risk to DoD assets.

INCREASINGLY CONNECTED PLATFORMS

The examples above represent three distinct attack access vectors against embedded systems: supply chain compromise (microprocessor compromise), maintenance pathways (vehicle USB), and compromising data links (broadcasted malware in TV signal). Current trends in weapons system platform modernization suggest that these same vectors are also applicable to defense platforms.

Most platforms are comprised of a diverse mix of commercial off-the-shelf, government off-the-shelf and custom hardware and software. Components have been developed over multiple iterations and many years. These components are sourced from a wide array of providers, each with different security practices. They leverage different processor types, operating systems, and source codes. Although this diversity may help improve the security of the system to prevent an attack from spreading [6], it also provides a large surface area for attackers to address, increasing the risk that they could establish at least a single point of presence via supply chain compromise.

Platforms also employ a range of data products throughout the course of their lifecycle to accomplish their mission. Flight-line maintenance activities, mission preparation, and post-mission analysis activities all involve connecting platforms to a variety of support equipment. These numerous pathways each create new opportunities for an attacker to gain presence or provide control.

Also like their commercial counterparts, platforms are increasingly interconnected via data links and tactical networks during mission execution. Connectivity via these links provides pathways that could extend attack impact beyond a single infected platform, by which sophisticated malware could propagate from one platform to another, or by which attackers could exert control over their payloads.

PARALLEL SECURITY APPROACHES

The trends of increasing computer automation and platform interconnectivity are here to stay, as they enable distinct tactical advantages. Platform security must improve to address these trends head on.

The two complementary approaches are common when it comes to traditional IT security measures. These apply in the world of defense platforms as well. The first is host-based security, where the security of the individual boxes on a network are improved to achieve increased security for the system overall. The second is network-based-security, where communications between hosts on a network are monitored to detect and potentially intercept malicious activity.

Build Secure

Improving the security of each subsystem on a platform is a great option and a necessary step in securing future platforms, but it's time-consuming and costly. There is certainly much to be gained through a thorough security review of each subsystem on a network, along with the implementation of bug fixes, configuration hardening, host-based security state monitoring, and other general security improvements. In many cases though, platform subsystems are not actively involved in current upgrades. Given the range of implementations present across all the subsystems on a given platform, there is no single silver bullet solution for host-based protection, such as a "platform antivirus" or the like. Instead, platform stakeholders should consider incorporating cybersecurity hardening requirements during subsystem upgrades, as informed by the outcomes of cyber risk assessments against their platform.

A Cyber Warning Receiver, designed to look for malicious activity on the 1553 bus can provide the broadly applicable solution necessary to achieve near-term game-changing platform security enhancement.

Network Lockdown

The actions necessary to conduct a cyber-attack, and the effects will, in the majority of cases, be observable via the data networks used to communicate commands, status, and data between systems on a platform. Although a compromised box could affect its function without leveraging any network communications, attacks against other system components will involve the use of platform networks. With this in mind, monitoring these networks for malicious activity can provide the situational awareness necessary to detect an attack and inform an appropriate response.

A common set of networks covers the vast majority of communications occurring on these platforms. In particular, the U.S. Army's Common Avionics Architecture System (CAAS) depicted in Figure 1 relies heavily on Ethernet and MIL-STD-1553 (or fiber optic 1773) networks, and also includes support for RS-232, RS-422, Arinc 429, analog and discrete signals [7].

Within a broad range of platforms employed by the Army and other services, 1553 networks form the backbone for communications between platform subsystems. They provide the critical link between pilot interface equipment like displays and keypads, and the endpoint devices that actually implement critical control or measurement capabilities. Monitoring the 1553 bus would provide a high degree of visibility into cyberattacks. A Cyber Warning Receiver, designed to look specifically for malicious activity on the 1553 bus can provide the general broadly applicable solution necessary to achieve near-term game-changing platform security enhancement. This device can be rapidly adapted to fit a range of platforms and provide immense benefit to the cyber security posture of the overall fleet.

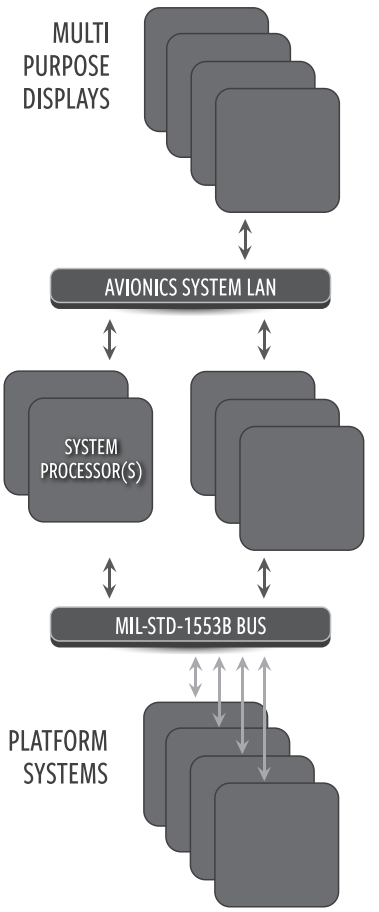


Figure 1: The Common Avionics Architecture System

THE MIL-STD-1553 NETWORK

MIL-STD-1553 is a serial messaging interface that prescribes a physical layer and data link protocol for exchange of data between a set of terminals residing on a bus. The physical network topology is flat, with all remote terminals (RTs) connected and listening to the same bus signal [8].

BC to Specific RT(s)	BC to All RT (Broadcast)
1. Controller to RT Transfer	1. Controller to RT(s) Transfer
2. RT to Controller Transfer	2. RT to RT(s) Transfers
3. RT to RT Transfers	3. Mode Command Without Data Word (Broadcast)
4. Mode Command Without Data Word	4. Mode Command With Data Word (Broadcast)
5. Mode Command With Data Word (Transmit)	
6. Mode Command With Data Word (Receive)	

Table 1: MIL-STD-1553 Message Types

All communications are facilitated by a single terminal designated as the Bus Controller. The Bus Controller implements a schedule on which it sends and receives information to and from the other terminals, or instructs them to pass messages between one another. Each message in the schedule is repeated at a prescribed rate, typically ranging from 50 times per second to once every two seconds. The bus also supports asynchronous messaging and supports polling for RTs that need to send an extra message on a given cycle. The 1553 bus is designed for determinism, reliability and redundancy, and comprises at least two redundant busses, and two redundant bus controllers (a primary and a backup) to enable failover in the event of a single failure conditions.

CYBER ATTACKS AND 1553

The breadth of published work on 1553 attacks is small in comparison to research for similar consumer, commercial, and industrial networks. Such networks are more openly accessible to security researchers for characterization. In particular, security research in the field of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems has illustrated the potential vulnerability of similar serial messaging interfaces. The MODBUS serial protocol, which has several features in common with 1553, has been the subject of extensive cyber security research. Huitsing, Chandia et. Al., in their paper describing attack taxonomies for Modbus Protocols [9], propose 15 distinct attacks across five classes for the Modbus serial protocol. Such findings are a useful starting point when considering the cyber security of 1553.

Through internal investment, we've adapted existing platform System Integration Labs to create a 1553 cyber security test bed. Using this as a research tool, we have begun to explore and characterize the space of 1553 attacks, considering attacks that directly target, exploit, or misuse 1553 functionality, and also attacks for which 1553 networks are involved, but not directly targeted. Our ongoing research has shown that many of the attack types conceived for other network types are also applicable to the 1553 network. The standard does not provide any security features, such as authentication or encryption that would mitigate such misuse.

The attack types available to an attacker exploiting the 1553 network depend on the specific foothold they achieve on a platform. In general, there are several positions an attacker might hold on a platform with respect to the 1553 system:

1. Attacker presence on systems outside the 1553 network that leverage data sent or received via the 1553 network;
2. Presence on a Remote Terminal connected the 1553 network;
3. Presence on a Bus Controller for the 1553 network; and
4. Multiple points of presence creating a combination of these states

Given this set of states, some of the attack types we've described and characterized are:

- Methods by which a compromised bus controller could impact the system. A compromised bus controller enables a high degree of control. It enables an attacker to initiate new messages, remove existing messages, or intercept and modify data in transit between remote terminals.
- Methods by which a compromised Remote Terminal could initiate new messages on the 1553 bus without coordination with the bus controller, impersonate a different Remote Terminal, or even attempt to become the bus controller.
- Methods by which any compromised host on the 1553 network could deny messaging between other remote terminals.
- Attacks in which basic rules and conventions of the 1553 standard, or the application layer data they contain, are violated.
- Attacks where a compromised host deliberately sends incorrect data to another host as part of the normal data exchange cycle. This could include measurement data, control commands, system status or other types of information.

Each of the attack types above have been hypothesized along with specific details relating to their realization on the 1553 bus. Some have been tested in practice. Discussion of these specific implementation details are beyond the scope of this article. Consideration of possible attack types and characterization of their effects helps inform a robust design for a platform security detection system like a Cyber Warning Receiver.

ATTACK OBSERVABLES

As the attacks described above take place on a 1553 network, they produce side effects that are observable to a high-fidelity bus monitor. For the purpose of organizing these observable side effects, the 1553 network can be considered as being comprised of several network layers, as depicted in Figure 2.

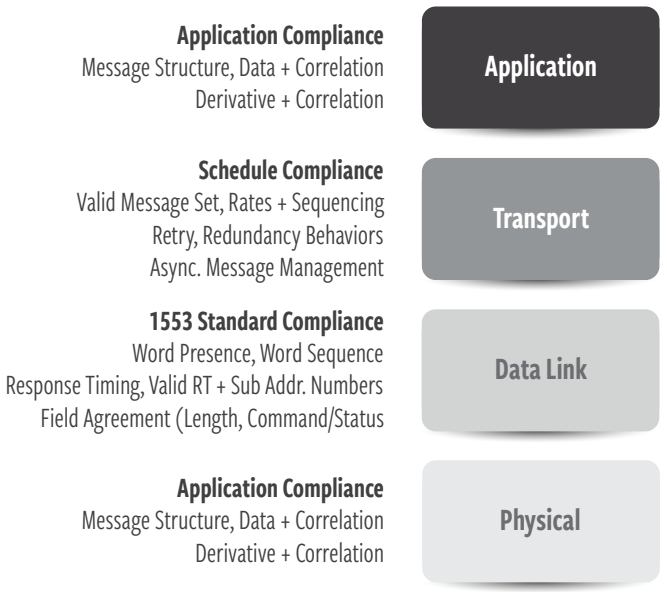


Figure 2: 1553 Network Layers and Observables

The bottom layer is the physical layer, which contains observables relating to the fundamental electrical environment necessary for proper operation of 1553. Certain attacks can cause disturbances at this level, especially in cases where misuse of the 1553 bus causes message collisions.

The next layer up is the data link layer, which covers low-level implementation details of the 1553 protocol. At this level, we can detect that only valid hosts and sub-addresses are present, and also that the expected message structure is intact, including the allowed message types and expected word sequences. Some attack types can cause changes to this ordering or produce multiple repeated copies of certain message words. The typical request and response timings for 1553 transactions can also be monitored at this level.

The next level up is a transport layer, in which platform specific attributes relating to the use of 1553 are defined. Messages that occur on 1553 can be uniquely identified by attributes including their type, source, destination and length. At this layer, we can verify that the system is using the set of messages expected to occur as part of the schedule, with the appropriate sequence and timing. Monitoring systems must account for changes to this schedule that may result from different operating modes for the platform. At this level, it's also possible to enforce that retransmit or redundancy features spreading messages across multiple busses are performing as expected without misuse.

The top level is the application layer. Details at the application layer are specific to the individual systems on the bus and their implementations. A navigation device may transmit one type of data using message formats and data representations established by its developers, while a threat warning system may use a completely different representation

for its data. Detection of a valid structure is one useful observable. Where data fields are specified or can be otherwise identified, a set of normal behaviors can be observed based on their values. For example, data may be known to have a limited range of values, to exhibit a known distribution, or to have a limited rate at which it can change. In other cases, multiple data fields might exhibit correlations, such as always moving together, or negating one another. Performance outside of these norms could be indicators for a cyber attack.

DETECTING ANOMALIES

A Cyber Warning Receiver operates by monitoring traffic and discovering anomalies in the behavior of these observations and measurements. The normal set of behaviors for each of the measurements must be characterized before deployment based on the 1553 specifications and specific inputs for the platform to be protected. Examples of specific input may include valid RT and sub-address ranges in use, and message schedule in different operating modes, and observations from collections of real world data.

In general, the higher the layer at which observation and characterization are required, the more specified a solution is to a particular attack, and the more data will be required to establish normal behavior and detect anomalies. Leveraging observable side effects that are agnostic to specific attack implementation details enables detection of attacks that have not before been observed in the wild, or preconceived by defenders. For lower layers, the number of possible attack approaches is limited, making it tractable for subject matter experts (SMEs) to explicitly define a spanning set of detectors. At these lower levels, detectors are also more portable than for higher levels. This simplifies the task of implementing cyber threat detection across platforms.

Although there are many advantages to monitoring the 1553 bus at lower levels, observations derived from these layers are not sufficient by themselves. There are important classes of cyber-attack that do not produce observable impacts at these layers. For example, manipulation of data from a given device would only be observable by changes in the platform-specific messages that exist in the application layer, as would violation of application layer message formatting. To characterize these forms of attack via the application layer, and detect them on-the-fly, more sophisticated anomaly detectors are required.

Creating anomaly detectors to operate at the application layer introduces several practical challenges:

1. Scalability to address the sheer volume of data relationships that would exist for all systems and messages across a complete defense platform. Do all of these relationships need to be enumerated by hand?
2. Managing the specifics of the application layer message formats and field locations for dozens of devices and hundreds of unique messages. Do these formats need to be manually specified to enable a practical system?

3. Discovery of subtle or secondary correlations that might escape the intuitions of human cyber defense experts and therefore remain open to exploitation by malicious parties.

These limitations suggest the use of more automated techniques for anomaly detector creation.

MACHINE LEARNING AS A KEY ENABLER

Given the typical platform, which contains multiple busses, each with multiple communicating 1553 devices sending multiple messages between one another, how can we equip detection systems with the ability to detect attacks occurring at the application layer? In short, a Cyber Warning Receiver must be programmed or trained to recognize how a system should behave under normal operating conditions, and how this behavior would manifest in the various observable measurements described above.

Advances in machine learning provide this capability. Machine learning also innately addresses the three challenges identified at the end of the previous section. Powerful parameter estimation and model structure detection techniques from machine learning are beneficial for system identification [10]. These capabilities help address the breadth of anomaly detection instances required to form a robust monitoring solution. Multiple examples of using observations to establish normal behavior models for complex systems exist [11]. Activity outside that expected by the normal behavior models is thus anomalous and becomes a data point for cyberattack investigation.

Modern machine learning approaches incorporate feature engineering and credit assignment as key elements. Deep machine learning techniques, for example, combine input observations (e.g., values in each 1553 message data field) into more abstract aggregate features that, while no longer representing actual physical measurements, provide an excellent basis for making decisions (i.e., normal behavior or not) [12]. Machine learning automatically selects which learned features contribute to making such decisions and which are essentially irrelevant—they assign credit to the various features. Over and above increasing the predictive power of the learned normalcy models, these characteristics of appropriate machine learning approaches obviate the challenge of identifying the most important data fields within the 1553 application layer. This is a huge benefit over the alternative of manual specification of data fields and their relative importance. Manual specification is cumbersome, especially considering that application layer message definitions may not exist in one place, but may be scattered across multiple disparate interface description documents, each utilizing different formats which makes them poorly suited to automated parsing.

Machine learning enables reasoning over much larger volumes of data than would be possible for human experts alone. Anomaly detectors increase the visible range of subtle

interactions and mutual patterns of behavior exhibited by disparate elements on the 1553 bus. These patterns may seem innocuous to cyber defense experts trying to envision attack vectors. However, these are exactly the oversights that inevitably get exploited. Finding instances of such subtle relationships has enhanced situational awareness in other domains [13]. Interestingly, insight into such patterns may also prove advantageous in system evaluation and trouble-shooting when non-attack anomalies surface.

Leveraging observable side effects that are agnostic to the specific attack implementation details enables detection of attacks that haven't before been observed in the wild, or preconceived by defenders.

By addressing the three challenges outlined above for reasoning about platform security using deep inspection of data at the application layer, machine learning is a key enabler for cyber situational awareness. Use of machine learning is not exclusive to the application layer, however, and is useful at the lower protocol layers as well. For example, machine learning algorithms can learn the normal message schedule for the platform as a function of the different operating modes, and/or establish normal electrical signal levels at the physical layer. Moreover, these adaptive algorithms can help eliminate the need for tuning and tailoring of detection systems for each instance of the protected platform. Instead, they enable deployment of solutions applicable across an entire platform fleet.

TRAINING FOR CONTINUED SUCCESS

With machine learning comes a need for algorithm training, the process by which machine learning algorithms ingest relevant data, extract features, and build their representations of expected behavior. For a practical defense system, this training should not impose intensive requirements for data collection. Suitable machine learning algorithms operate initially with bus data recorded during field trials and qualification testing and improve their performance upon acquisition of additional data.

One avenue for the collection of additional training data involves incorporation into the mission cycle for a given platform. Bus-recordings collected post-mission would support incremental updates to training sets and learned behavior models. Distributing new models across platform instances at regular intervals enables all protected platforms to benefit continuously from learning over collective data. With more data and collective knowledge, the performance of these machine learning based systems would continue to improve, providing a defense system that evolves with new threats, and adapts to defeat them.

MEASURING MALICE

Not every anomaly means the platform is under attack. Systems are regularly entering and exiting new states and scenarios and experiencing abnormal conditions resulting from a range of incidental activities or failure modes. The key distinction between system glitches and cyberattacks are the correlations that exist between observations, and the story they tell.

Any single cyberattack step would generate a set of measurable side effects and artifacts. Multiple steps in sequence begin to form a picture of the current attacker presence and their objectives in an attack.

A data fusion system is the key element required to put these pieces together. Data fusion formulates the best possible estimate of the underlying system state based on observations, then determines the likelihood that anomalies are caused by an underlying failure, engagement in a scenario or operating mode not previously characterized, or a cyberattack.

BUILDING A COMPLETE PICTURE

A final consideration in defining a Cyber Warning Receiver capability is the question of appropriate output format. The output should never distract a pilot or other key mission personnel unless the findings suggest an imminent survivability threat. Coordinated cyber and kinetic attacks in a combat situation would need to be prioritized to ensure a manageable feed of critical information to the operator.

There is still work to be done to establish the exact manner in which a platform and its occupants should respond in the face of a cyber threat. To follow a general model, this would mean informing or alerting operators given the high probability of compromise for a mission critical system, or if the attack trajectory suggests movement in that direction. Providing too much information, or generating excessive nuisance false alarms might be cause for an operator to disable a system, eliminating the protection and defeating the purpose.

The key distinction between system glitches and cyberattacks are the correlations that exist between observations, and the story they tell.

Another key feature of a Cyber Warning Receiver is the operator interface, which allows operators to explore underlying system security state, and examine the evidence supporting those assumptions. Such data could be analyzed outside of critical moments to enable early detection of malicious actors, or activities relating to the initial establishment of cyber presence on the platform.

Finally, a Cyber Warning Receiver can provide the capability to perform post-mission forensic analysis of anomalous data, in order to provide better threat insights and

preparedness for future engagements. This is enabled by capturing and recording the raw data that is deemed anomalous.

ACTIVE DEFENSE

A major decision to be made with respect to Cyber Warning Receiver technology is the location and configuration of the unit within the system. Two possibilities exist: active or passive.

Cyber warning capabilities form a key addition to the suite of platform survivability equipment, providing visibility into the cyber domain and keeping the warfighter safe in the face of this emerging advanced threat.

The first possibility is to configure a cyber-warning receiver as a passive device, monitoring the system for malicious activity and alerting operators of anything suspicious, but never actively interacting with the network. In this case, the device would need to be positioned within a system to enable monitoring of all applicable buses. This is analogous to the Intrusion Detection System concept from traditional IT security. This option provides a degree of safety from a regression test standpoint, and the likelihood of any performance impact of a Cyber Warning Receiver on critical mission activities is minimized.

Alternatively, a Cyber Warning Receiver could be positioned in line with critical 1553 bus subsystems, prepared to take rapid and decisive action to stop cyber-attacks in their tracks. Given that cyber-attacks can happen in the blink of an eye, active defense may in some cases be the only reasonable way to stop an attack from occurring. The risk with an inline device is that it could be tricked by attackers into providing an inappropriate response, in effect becoming a part of the attack itself. Design precautions would be necessary to ensure that attack suppression actions delivered by an inline Cyber Warning Receiver could not create consequences beyond what the original attack would have achieved by itself.

Given its role, and especially when considered as part of an active defense configuration, a Cyber Warning Receiver as envisioned might itself become an attractive target for adversaries. As the core of cyber security operations on a platform, attackers may make it a priority to disable or interfere with this system to enable their other objectives. As such, any Cyber Warning Receiver would have to be built with the utmost secure design in mind. This could include applying provable security approaches, or leveraging security hardened hardware and software through an active security development lifecycle that includes regular software patching.

CONCLUSION

Modern weapons platforms continue to reach new heights of interconnectivity and software-defined automation. With these enhancements comes the need to address the increasing cyber security risks. Evidence from the commercial and industrial sectors suggests that many of the access vectors and attack methods observed there also apply to DoD platforms, with consequences that are potentially much more severe. Despite this reality, many modern weapons system platforms currently operate without any means of providing detailed situational awareness into their cyber security state.

Platform stakeholders should consider a two-pronged approach to improving platform cyber security posture. This approach begins with implementing survivability equipment that can monitor platform networks for malicious activity. Network monitoring enables near-term capability to detect or prevent cyber-attacks that are a very real threat today. The second facet of this approach involves making ongoing security improvements to individual subsystems, which will help reduce the overall platform attack surface over time.

The MIL-STD-1553 bus is identified as a prime location for observing cyberattacks in progress. This bus is pervasive across both modern and legacy defense platforms and forms the backbone for an exchange of commands, status, and data between operators and the critical subsystems essential to the function of a platform. Cyber Warning Receiver technology can monitor this bus for a range of malicious activities and attack types. This includes attacks that are being carried out to exploit the 1553 bus itself and also attacks that cause deviation from established system behavior norms for data traversing this bus.

Through continuing research, we have characterized a wide range of 1553 network-based attacks and established a corresponding set of observables. A Cyber Warning Receiver measures these observables over time and identifies anomalous or malicious activity. It implements detectors from two categories: explicit detection rules defined by subject matter experts, and system behavior models derived using machine learning. Use of explicit detection rules enables monitoring of the 1553 physical and data link layers for anomalous activity that violates the 1553 standard or does not agree with basic attributes of the known system configuration. The use of learned system behaviors enables deep inspection of messages traversing the 1553 interface to verify they are operating on schedule, that the expected correlations exist between various data fields, and that data ranges and rates of change are within their expected values.

When a cyberattack occurs, the observations and anomalies that result are collected and examined using a data fusion process. This process estimates the underlying security state of the platform and tracks attacker actions. When critical systems are involved, or a survivability risk is identified, a Cyber Warning Receiver can alert operators. Cyber warning capabilities form a key addition to the suite of platform survivability equipment, providing visibility into the cyber domain and keeping the warfighter safe in the face of this emerging advanced threat.

NOTES

1. Doug Gross, 2013, Foul-mouthed hacker hijacks baby's monitor, August 14, http://www.cnn.com/2013/08/14/tech/web/hacked-baby-monitor, (accessed April 25, 2017).

2. Dan Goodin, 2017, Smart TV hack embeds attack code into broadcast signal—no access required. March 31, https://arstechnica.com/security/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/(accessed April 25, 2017).

3. Charlie Miller and Chris Valasek, 2015, "Remote exploitation of an unaltered passenger vehicle." Black Hat USA 2015.

4. Nicolas Falliere, Liam O Murchu, and Eric Chien, 2011, W32.Stuxnet Dossier Version 1.4. Malware Analysis, Symantec.

5. Bill Gertz, 2016. The military is concerned that Chinese computer products could pose a cyber security threat, October 24, http://www.businessinsider.com/pentagon-chinese-computer-products-cyber-security-threat-2016-10, (accessed April 25, 2017).

6. Per Larsen, Stefan Brunthaler, and Michael Franz, 2014, "Security through diversity: Are we there yet?" IEEE Security & Privacy 12, no. 2 28-35.

7. Paul Clements and John K. Bergey, 2005, The U.S. Army's Common Avionics Architecture System (CAAS) Product Line: A Case Study. Technical Report, Pittsburgh, PA: Carnegie Mellon Software Engineering Instutute.

8. Wikipedia Contributors. n.d., "MIL-STD-1553," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=MIL-STD-1553&oldid=776707274, (accessed April 25, 2017).

9. Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi, "Attack taxonomies for the Modbus protocols.," International Journal of Critical Infrastructure Protection 1 (2008): 37-44, doi:10.1016/j.ijcip.2008.08.003.

10. Lennart Ljung, Hakan Hjalmarsson and Henrik Ohlsson, 2011, Four encounters with system identification. European Journal of Control, 5-6, 449-471; Pillonetto, Gianluigi, 2016, The interplay between system identification and machine learning, arXiv:1612.09158v1.

11. B.J. Rhodes, N.A. Bomberger, M. Zandipour, D. Garagic, L.H. Stolzar, J.R. Dankert, A.M. Waxman, & M. Seibert, 2009, Automated activity pattern learning and monitoring provide decision support to supervisors of busy environments, Intelligent Decision Technologies, 3, 59–74; B.J. Rhodes, N.A. Bomberger, M. Zandipour, L.H. Stolzar, D. Garagic, J.R. Dankert, & M. Seibert, 2009, Anomaly detection & behavior prediction: Higher-level fusion based on computational neuroscientific principles. In N. Milisavljević (Ed.), Sensor and Data Fusion, 323–336, Croatia: In-Teh.

12. Y. Bengio, A. Courville, and P. Vincent, 2013, Representation learning: A review and new perspectives. IEEE Trans, PAMI (Special issue: Learning Deep Architectures), 35, 1798–1828, doi:10.1109/tpami.2013.50; Hinton, G. E.; Salakhutdinov, R. R. (2006), Reducing the dimensionality of data with neural networks. Science, 313 (5786), 504–507, doi:Y. 10.1126/science, 1127647.

13. M. Zandipour, B.J. Rhodes, and N.A. Bomberger, 2009, Probabilistic prediction of vessel motion multiple spatial scales of maritime situation awareness, In Proceedings of the 10th International Conference on Information Fusion, Cologne, Germany, June 30–July 3, 2008; J.R. Dankert, M. Zandipour, N. Pioch, B. Biehl, R. Bussjager, C.Y. Chong, M. Schneider, M. Seibert, S. Zheng, & B.J. Rhodes, (2010), MIFFSSA: A multi-INT fusion and discovery approach for Counter-Space Situational Awareness, In Proceedings of 2010 Space Control Conference (SCC), Lexington, MA, USA, May 1–3, 2010.

Making the Point—West Point's Defenses and Digital Age Implications, 1778–1781

Dr. Nicholas Michael Sambaluk

ABSTRACT

Despite obvious distinctions, parallels exist between 18th century era fortification and the purposes, processes, and implications of pursuing security in an artificial cyber realm of the 21st century. The Revolutionary War era fortification of the Hudson River bottleneck focused upon the West Point area between 1778 and 1781. Differing professional perspectives and factors such as available resources led to disagreement about the defensive concept, and Thaddeus Kosciuszko's construction of layered defenses strengthened the US position in the region during the latter phases of the war. British failure in a belated overland raid, demonstrating an inability to "brute" the new defenses, led to British interest in leveraging an insider threat (Benedict Arnold), but then as now, insider threats could not automatically guarantee success.

INTRODUCTION

History leverages evidence and analysis to create meaningful ways to understand the past and develop wisdom to use in the present. Because every situation is distinct and unrepeatable—and yet the need for comparison is a useful tool for human beings as pattern-learners—the earnest exploration of nuanced analogies provides a chance to step back from the details of a contemporary issue for a clearer understanding of how to handle problems and utilize opportunities. Fittingly, when the US Army established its undergraduate Academy at West Point, its history department adopted the motto "wisdom through history."

AN OPPORTUNITY AND A VULNERABILITY

Within six weeks of the first fighting in the American Revolution, American policymakers had identified the need to defend the Hudson River from superior British naval

Dr. Nicholas Michael Sambaluk is an Associate Professor of Comparative Military Studies at the Air Command and Staff College at Maxwell Air Force Base. He taught military history at Purdue University during the 2015-16 school year and served as a Liaison for Cyber Research for the Army Cyber Institute at West Point from 2014 to 2016. From January 2013 through May 2015, he served on the USMA history department faculty. His first book, *The Other Space Race: Eisenhower and the Quest for Aerospace Security* (Naval Institute, 2015), explored the pursuit of effective security policy, and his writing also appears as part of *Cyber Warfare: A Reference Handbook* (ABC-CLIO, 2015) and in the journal *Cold War History.*

power. A length of the river forty miles north of New York City offered some intriguing opportunities for fortification: bends in the river could slow down enemy ships at specific points between Verplanck in the south and West Point in the north. On this ten-mile stretch, American militia and a civilian architect had constructed three crude fortifications. Poorly sited, short of labor, and lacking the heavy caliber artillery needed to threaten warships on the river, the forts proved easy meat to a British contingent that advanced north toward Major General John Burgoyne's embattled army at Saratoga. The limitations of 18th century communication prevented better coordination between British forces, and the withdrawal of the Hudson River force to winter quarters and the capitulation of the northern force in upstate New York were the only reasons that the British did not gain control of the Hudson River in the summer and fall of 1777.

Well before the crisis of 1777, the river's strategic importance (and vulnerability) had been identified. One officer wrote the Continental Congress' president to report that "it has become a matter of important consideration how to remedy the evil" of "the Enemy ... possessing the Navigation of the North [Hudson] River and rendering the communication & Intercourse between the States divided by it, extremely hazardous & precarious." [1] Americans generals George Washington, George Clinton, and William Alexander (Lord Stirling) had realized the need to fortify the bluff on the west bank of the river across from the feeble but expensive Fort Constitution at the northern edge of the river's defense corridor. [2]

Recognizing that "upon the possession of the North River depends the security of all the upper part of the Government of New York, and the communications between the Eastern middle and southern

States," [3] Washington was certain of the river's strategically vital roleboth as a conduit and as a source of vulnerability. After British abandonment of the area, a new American committee reconnoitered the river valley and concluded that "the most proper place to obstruct the navigation of the river is at West Point." [4]

Image 1. Picturesque, but constrained: Fort Constitution's vantage. Photo Credit: Dr. Nicholas M. Sambaluk

SECURITY CONCEPTS

Defenses need to follow a single, coherent overall concept. Unfortunately, whereas the overarching problem from 1775-77 had been that the identification of a strategic vulnerability was not matched by technical talent that could answer the need, in 1778 there were multiple experts at work, and consequently a collision of "authorities."

Captain Lewis de la Radiere, a professionally trained military engineer, had arrived from France prior to official French involvement in the war. La Radiere had been charged by Washington, at the height of the Hudson crisis, with building river defenses; the precise wording (but not the spirit) of the order permitted la Radiere to focus myopically on reconstructing Fort Montgomery, a low-lying and assailable spot where Popolopen Creek joins the Hudson. Despite Governor Clinton's orders that "Col. La Radiere accommodate his plans & Mode of constructing the Batteries & Forts, to the Nature of the Country and Materials, Time & Number of Men," la Radiere quickly left issues of cost and constructability by the wayside, forgetting that the craftsmen his projected fort required were not in great supply in the Hudson Valley or upstate New York. [5] La Radiere's was a particularly unfortunate selection because the previous designer had already gone threefold over the allocated budget for fortifying the region, and he had thereby endangered the completion of any meaningful positions to guard the river.

La Radiere's resistance is all the more surprising when it is remembered that the Congress's weakness placed the responsibility for the river's defense on New York, that Governor Clinton had been urging planners to align their designs with the resources that could be delivered, and that Clinton had even described in some significant detail the concept for the proposed fort:

> I am clearly of Oppinion [*sic*] that a strong Fortress ought to be erected ... at the West Point opposite Fort Constitution ... as the most defensible Ground and because the Navigation of the River there is more difficult & uncertain and the River something narrower ...[.] A new Chain should be procured (if possible) & with the Boom which is nearly completed [*sic*] stretched across the River ...[.] It might be of great Advantage to erect a small strong Work on the high Point on the opposite Shore a little above Fort Constitution. [6]

Although the professional soldier of the 18th century was not an analog to the military professional of the 21st, George Clinton was a general principally due to his role as a politician. He was certainly not a trained military engineer, yet his overall description of a defensive work at West Point would make a more formidable fortification than Forts Clinton, Montgomery, and Constitution had collectively been during the British offensive in 1777. Perhaps the disappointing experiences of the previous campaign had taught the governor something about defending the river. For his part, la Radiere reacted to guidance by rejecting the decision of the committee and of the governor, petulantly writing to General Washington that he had "reasons" for dismissing their ideas, and pretentiously offering that "if I can Spair [sic] time in two or three weeks I will rid [sic] to the Head quarter and give [General; Washington] a Larger account of the Future Situation of this River when a fort will be constructed." [7]

Parallels exist between 18th century era fortification and the purposes, processes, and implications of pursuing security in an artificial cyber realm of the 21st century.

By this point, la Radiere's fellow officers were all too glad to allow him the opportunity to ride off to General Washington, thus unburdening themselves of him for long enough to proceed along their own design. Major General Israel Putnam communicated to Washington that "it was the Opinion of all except the Frenchman [la Radiere], that it was the best, and the only effectual [place] on the River" to defend. The cantankerous attitude of la Radiere, and the sheer impracticality of the scale of fortress he intended to build, contrasted starkly with the bearing of another military engineer on the scene. Thaddeus Kosciuszko had arrived from Poland in August 1776, having undertaken the bold

passage at his expense to fight alongside the rebels. Propelled by nationalist sentiment, Governor Clinton recommended Kosciuszko to the brigadier overseeing construction as "an Ingeous [sic] Young Man & disposed to do every Thing he had in the most agreeable Manner." [8]

Perhaps in part because of his longtime acclaim, Kosciuszko has faced recent revisionist critique as having played an overestimated part in American independence. [9] This revisionist effort appears to be both unfair and inaccurate. During the 18th century, military engineers were seen as specialists useful in building (or besieging) fortresses, but they were not typically granted the responsibility, authority, or respect of a line officer. This was patently the case in the French army, and evidence appears within the Revolutionary American army of this as well. [10] The point that Kosciuszko received only a single slight wound during the war (due to an errant friendly bayonet) entirely misses the fact that the nature of his skills meant he belonged away from battlefields. Furthermore, the rarity of those skills on the American side meant that a commander recklessly sending him into needless danger would also have been putting the national cause at inordinate risk. It furthermore does not account for Kosciuszko's effective service with General Horatio Gates's army against Burgoyne, or Gates's interest in having the Polish engineer returned to his field army in the fall of 1778. [11]

In his capacity as an 18th century military engineer, his talents were best employed either in designing a siege against an enemy fortress or in creating and overseeing the development of a fortified network. Strategy is the art of establishing plans that will achieve national objectives, doing so with the resources (including human, physical, fiscal, time) available. Kosciuszko devoted a similar sense of awareness when he began to design West Point's new generation of far more formidable defenses.

Image 2. A commanding view from Ft Putnam. Photo Credit: Dr. Nicholas M. Sambaluk

In his capacity as an 18th century military engineer, his talents were best employed either in designing a siege against an enemy fortress or in creating and overseeing the development of a fortified network. Strategy is the art of establishing plans that will

achieve national objectives, doing so with the resources (including human, physical, fiscal, time) available. Kosciuszko devoted a similar sense of awareness when he began to design West Point's new generation of far more formidable defenses.

LAYERED DEFENSES

The key was to establish a layered network structure. Whether dealing with cyber-security or medieval city walls, a single perimeter barrier may give a sense of security that is more comforting (and misleadingly safe feeling) than it is a guarantee of security. Observing the terrain, Kosciuszko, like some of his colleagues by 1778, recognized that there was no truly ideal location to use as a gun platform against targets traveling on the river. At best, there were semi-compromised positions.

Constitution Island sat on an isolated spit of land, separated by a boggy swamp from the east bank that did not preclude overland attack. Even more seriously, artillery positions on Constitution Island faced only the slim bow of oncoming ships, and therefore defenders could not fire effectively against enemy vessels until ships had already accomplished one of the two tight turns. This meant both that the enemy would have traversed half of the difficult geography (the very reason that this area had been chosen for fortification) and the modest American fort would be subjected to the more powerful broadside cannonade of a British warship.

One of the advantages of a layered network defense is that, with appropriate forethought and planning, initial positions can constitute an early degree of security

On the stretch between what is now North Dock and the West Point Clinton Soccer Field at the United States Military Academy, the situation was basically complementary to that of Constitution Island, except the elevation was a bit lower and enemy ships would be in the process of passing the final turn in the river as they came up to bludgeon a defending fortress. Narrow artillery positions might be built across the river from Fort Constitution, if it could be guaranteed that the bluffs above them would not be occupied by the enemy.

The answer was to develop a layered, networked defensive structure. Artillery at the Water Battery and Greene's Battery stood guard over the river at West Point, positioned just to the south of the western anchorage of the Great Chain. The Chain would be an additional obstruction to compel enemy vessels to stop, disembark sailors to clear the obstacle (under fire) before the ships could then continue to navigate the two close bends in the waterway. The Chain's eastern anchorage, on Constitution Island a few hundred feet from the traces of Romans' first efforts, would gain some protection from the building

of a small number of redoubts, semi-enclosed positions for small garrisons of infantry and potentially armed also with cannon. Thus, with these positions, the Hudson River itself was protected.

The extensive interlocking positions which secured the river defenses were key to the plan's strength. Adjacent to the West Point Plain Kosciuszko planned Sherborne's Redoubt and a larger fully enclosed position for artillery and infantry. These fortified areas would prevent an enemy from landing troops downriver and marching them overland onto the bluffs that would cause the river defenses to crumble. More specifically, the presence of these fortifications would deny speed or stealth to the enemy. As fortifications, they were to buy time to react and respond.

Kosciuszko had by this time spent a year and a half amongst the rebel forces and had some familiarity with the fiscal material weighing on the states and their armies. Kosciuszko's envisioned bluff defenses were considerably less extensive than the enlarged Fort Montgomery that la Radiere insisted upon. Kosciuszko's defenses could also be built more easily, more affordable, and potentially faster. Time was vital, as Kosciuszko recognized and as la Radiere had been told: "if we remain much longer disputing about the proper place, we shall lose the Winter, which is the only time that we have to make preparations for the reception of the Enemy" that Washington expected to return in the spring.[12] A half-built fortress is not half as good as a complete one, and without being able to know when an enemy might attack, building an initial capability that could expand with time proved a wiser alternative to the slow and potentially interrupted construction of a colossus whose integrity was moot until completion.

One of the advantages of a layered network defense (then and now) is that, with appropriate forethought and planning, initial positions can constitute an early degree of security and subsequent interlocking positions can be expeditiously constructed to further enhance the credibility of the complex.

Image 3. Fort Putnam, a key to the Hudson River's defenses. Photo Credit: Dr. Nicholas M. Sambaluk

RESILIENCE

In the case of West Point, the Water Battery and Greene's Battery guard the river, the bluff positions near the Plain protect the gun batteries, an enclosed Fort Putnam would be built on an overlooking hill to impede enemy overland access to the bluff's defenses, and then a series of redoubts and battery positions studding the hills and approaches to the west and south of Fort Putnam would come to constitute the balance of what is meant by the term "West Point fortifications." In all, these make up dozens of prepared positions on both sides of the Hudson River.

Social engineering in both physical and other environments like cyber is a completely relevant avenue even without the foreclosure of other options.

It was his attention to the interrelated issues of ease, affordability, and speed of construction that underscored the extent of Kosciuszko's contributions to American defense of the Hudson Valley. The education for military engineers in 18th century Europe followed in the footsteps of Sebastien de Vauban, whose works across France's frontiers display an appreciation for the uses of artillery, geometry, and advantageous use of geographic features. Kosciuszko's interlocking network was an artful application of established and proven principles, and the result secured the back door into New England from easy enemy incursions.

La Radiere intended to force Washington to grant him authority over the Hudson defenses (despite the fact that Kosciuszko's date of commission in the US Army was more than a year ahead of his own); construction at West Point proceeded because of his absence, and as 1778 gave way to 1779 and 1780, the fortresses and redoubts took shape, and the Great Chain was constructed for its seasonal emplacement following the Hudson's thaw and before its winter refreeze.[13] Another French officer, Brigadier General Louis Duportail, critiqued some of the particulars of Kosciuszko's design, but Washington's response was to initially direct Kosciuszko to make recommended modifications rather than to overhaul the new defensive concept.[14] The development of Kosciuszko's robust defenses presented would be British conquerors of the river with a much more difficult problem than they had faced in 1777.

The strengthening of West Point coincided with the shift of the war's main focus to the southern colonies and the campaigns that would culminate at Yorktown in 1781. The British force in New York City remained formidable, and the Empire remained interested in controlling the Hudson. British actions in the Hudson Valley region included a foray which got to within twelve miles of West Point when it reached Stony Point in July 1779.

Washington parried this move by dispatching a contingent of light infantry, referred to as the Light Infantry Corps, under the command of Brigadier General Anthony Wayne. His troops conducted an impressive night march, which in an era centuries before night vision or geolocation managed to find and reach the British force, which it promptly defeated in a small but significant battle.

Wayne's rebuff of the British at Stony Point indicated that the American military presence in the Hudson Valley was one that could not be dislodged as easily as Henry Clinton had managed two years before. Word of the crystallizing defensive construction and the ongoing strategic significance of the waterway did nothing to mitigate the negative implications of this realization. Increasing British resources were tied down both in holding New York City and in seeking to root out rebels in the south and raise loyalist sentiments there; additionally, the war's growing scope meant that by mid 1779 Britain fought against not only the rebellious colonies of the Atlantic seaboard but also against the French, Spanish, and Dutch Empires. These factors, including the enormously improved character of American Hudson River fortifications, drove British officers in America to recognize that their own Empire's military and naval forces were too hard pressed to organize a major renewed thrust against the Hudson in the foreseeable future.

INSIDER THREAT

As is often the case in physical and cyber environments, when it proves impracticable to brute through a defensive structure, and when deciphering its exploitable weaknesses does not seem an available alternative either, social engineering remains a potential option. In fact, social engineering in both physical and other environments like cyber is a completely relevant avenue even without the foreclosure of other options. Britain had a social engineering target in mind: a second tier American hero who had gained some early notoriety earlier in the war by exploits including the cooperative capture of the inadequately alert defenses at Fort Ticonderoga and the perceptive thought of redeploying the fort's cannon to arm American forces in Boston and on the Hudson. Seizure of the fort also facilitated an abortive expedition to Canada to invite French Canadian partners into the rebel fold. Little in the way of active rebel sentiment emerged from the French Canadians, who had been proactively accommodated by Major General James Murray and his successor Sir Guy Carleton between the Seven Years War and the American Revolution.[15] The disappointing Canadian

> Spear phishing and similar vectors will not guarantee success, even a willing partner in the mold of Benedict Arnold is not a guarantee for victory.

response was matched by the excruciating experience of the American expedition itself, and Benedict Arnold led the survivors on a forced march back across the Canadian border and through upstate New York,[16] where bitter winter temperatures and fiercely low rations competed in brutality, driving soldiers to contemplate eating their ragged footwear and go barefoot or march through snow with thin shoes and empty stomachs.

Arnold's exact motivations went with him to the grave. He certainly was a soldier who committed numerous heroic acts during his complicated career. Since he broke with the British Empire to become a rebel and then abandoned the revolutionary cause to become a Tory commander, his loyalty could not by the end of the war be fully trusted by anyone. This was particularly the case since the considerations which precipitated his second turn of allegiance coincided with the British offering him cash in exchange for the plans to West Point's defenses, and leveraging his position to raise the price higher before sealing the bargain.

Despite the allure of unleashing insider threats upon an adversary, the results are not necessarily effective.

Regardless of whether Arnold's motives were purely venal and materialistic, or a realtered sense of patriotic duty or an impression that he could orchestrate reconciliation at the close of a doomed conflict is beyond the scope of this study. His efforts to betray the defensive positions guarding the Hudson speak to the threat that social engineering and insider threats pose, in physical as well digital realms. Complex motivations and insider status can also impede tracking and attribution of these threats.

CONCLUSIONS ABOUT SECURITY

The defense of the Hudson River from 1778 through 1781 teaches some important points which are relevant to security in other contexts and environments, including the cyber arena. One issue is that defensive arrangements, like strategic plans, need to follow a single and coherent overall concept. It is tempting, but misleading, to portray a competition between la Radiere and Kosciuszko—a simple struggle between two expert engineers. The record demonstrates that many officers by the winter of 1777-8 had come to recognize the importance of West Point in defending the river. La Radiere attempted to ignore and bypass this (correct) consensus of nonprofessionals. Kosciuszko was aware of the importance of defending West Point and that the successive hills overlooking West Point complicated the defensive task. Kosciuszko's accomplishment was that he developed a sophisticated solution that used the numerous hills to turn the dilemma back onto an attacker since the new layered defenses formed a succession of obstacles to overcome.

Impressively, Kosciuszko's defensive concept not only turned the complex terrain into an advantage but also made timely use of the materials and labor that was available. Effective defenses are those that can buy vital time for defenders and can do so while using the resources (human, physical, fiscal, and chronological) that are appropriate and available. Kosciuszko's defensive concept was also one which could be improved over time, without having to fundamentally change in concept. This was vital in the midst of a long war, where a latent enemy threat was consistently within forty (and often fewer) miles of the fort system. The parallels here with maintaining security in a cyber environment are palpable.

A final area in which the physical defense scenario of the Hudson River and the multifaceted cyber arena are similar is in the problem of the socially engineered threat vector. When the British realized that conventional campaigns in the style of 1777 were too logistically demanding to undertake in the latter phases of the war, and that smaller raids toward Stony Point could be smashed before reaching the West Point forts, the British reached for a timeless method of undermining a defensive position; turning an enemy insider into a covert ally. Despite the allure of unleashing insider threats upon an adversary, the results are not necessarily effective. Benedict Arnold's failure speaks to some of the challenges that are involved in this route. Spear phishing and similar vectors will not necessarily guarantee success, and even a willing partner in the mold of Benedict Arnold is not a guarantee for victory.

Arnold's treachery caused tension and concern—unease and instability—among the Americans. It did not accomplish the British objective of regaining the Hudson. Upsetting the enemy's plans was something more possible in the fall of 1780 than accomplishing one's own goals. And that is something that has always been true in war.

NOTES

1. Lieutenant Colonel Robert Hanson Harrison to John Hancock, October 25, 1776, *The Papers of George Washington: Revolutionary War Series 7, October 1776-January 1777,* ed. Philander D Chase (University Press of Virginia, 1997), 29.

2. Footnote 6, *The Papers of George Washington: Revolutionary War Series 7,* 143.

3. To Major General Horatio Gates [from George Washington], December 2, 1777, *The Papers of George Washington: Revolutionary War Series 12, October-December 1777,* ed. Philander D Chase (University Press of Virginia, 2002), 497.

4. Footnote with January 14, 1778 committee report, *Public Papers of George Clinton, First Governor of New York, 1777-1795 – 1801-1804, Volume II* (New York: Wynkoop Hallenbeck Crawford, 1900), 679.

5. To Major General Horatio Gates [from George Washington], December 2, 1777, *The Papers of George Washington: Revolutionary War Series 12,* 497-8. "Defenses at West Point," March 5, 1778, *Public Papers of George Clinton, Volume II, 848.* Charles E. Miller, Donald V. Lockey, and Joseph Visconti, *Highland Fortress: The Fortification of West Point During the American Revolution, 1775-1783* (United States Military Academy, 1979), 57-9, 69.

6. From George Clinton [to George Washington], December 20, 1777, *The Papers of George Washington: Revolutionary War Series 12,* 646-47.

7. From Lieutenant Colonel La Radiere [to George Washington], January 13, 1778, *The Papers of George Washington, Revolutionary War Series 7, October 1776-January 1777,* ed. Philander D. Chase (University Press of Virginia, 2003), 225.

8. George Clinton to Samuel Parsons, March 26, 1778, *The Public Papers of George Clinton, First Governor of New York, 1777-1795 – 1801-1804, Volume III* (Albany: James B Lyon, 1900), 86.

9. David Levine, "The Influence of Tadeusz Kosciuszko, Marquis de Lafayette, and Friedrich Von Steuben," *Hudson Valley* http://www.hvmag.com/Hudson-Valley-Magazine/January-2015/The-Influence-of-Tadeusz-Kosciuszko-Marquis-de-Lafayette-and-Friedrich-Von-Steuben/.

10. Janis Langins: *Conserving the Enlightenment: French Military Engineering from Vauban to the Revolution* (MIT, 2004); "Defenses at West Point," March 5, 1778, *Public Papers of George Clinton, Volume II, 848.*

11. Kosciuszko's service throughout the war, including the later campaigns in the south after his fortifying West Point, earned high praise from American colleagues. From Major General Horatio Gates [to George Washington], September 11, 1778, *The Papers of George Washington: Revolutionary War Series 16, July-September 1778,* ed. Philander D Chase (University Press of Virginia, 2006), 574; Miecislaus Haiman, *Kosciuszko in the American Revolution* (New York: Policy Institute of Arts and Sciences in America, 1943), 142.

12. *The Papers of George Washington: Revolutionary War Series 13, December 1777-February 1778,* ed. Philander D Chase (University Press of Virginia, 2003), 342.

13. Theodore J. Crackell, *West Point: A Bicentennial History* (University of Kansas, 2002), 13.

14. Wash Sixteen, 594-98. Wash Seventeen, 46. Francis Casimir Kajencki, *Thaddeus Kosciuszko: Military Engineer of the American Revolution* (El Paso, TX: Southwest Polonia Press, 1998), 97.

15. Willard Sterne Randall, *Benedict Arnold: Patriot and Traitor* (New York: William Morrow and Company, 1990), 87, 95.

16. Holly A. Mayer, "Canada, Congress, and the Continental Army: Strategic Accommodations, 1774-1776," *The Journal of Military History 78.2* (April 2014), 513.

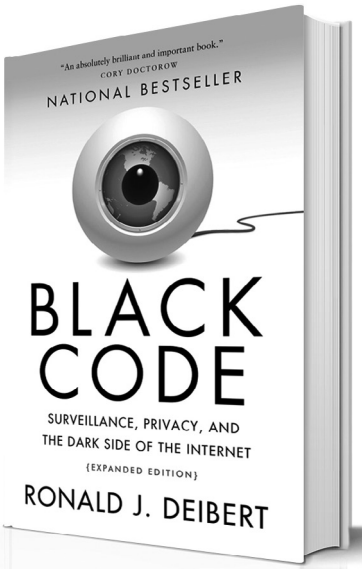
17. Randall, *Benedict Arnold,* 188-89, 233-37.

The Cyber Defense Review

Book Review

Black Code: Surveillance, Privacy, and the Dark Side of the Internet by Dr. Ronald J. Deibert

Reviewed by CDT Monte Ho
and Dr. Jan Kallberg



Dr. Ronald J. Deibert's book *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* addresses growing concerns regarding international cyber threats and argues against current countries' methods of responding to these threats. Deibert presents a solid, well-rounded argument, with intriguing evidence to support his assertions regarding our flawed cybersecurity environment, and closes *Black Code* with personal recommendations to secure and regulate the cyberspace domain. Readers receive a broad spectrum analysis of cyberspace and cybersecurity and are provided specific information on the actions and interactions of hackers, international governments, and related cyber industries. *Black Code* reads like a cyber novel; brilliantly crafted with a strong foundation and argument against current cybersecurity techniques and practices. Dr. Deibert is Professor of Political Science, and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is described as "an interdisciplinary research and development laboratory working at the intersection of the digital technologies, global security, and human rights."

Dr. Deibert opens *Black Code* with a revealing description of his background as a researcher at the Citizen Lab and a detailed accounting of how modern cyberspace is defined. The first few chapters give readers a baseline knowledge of the physical and theoretical components of cyberspace, and how these pieces, functioning together, provide the entirety of the Internet. He then provides compelling facts and in-depth analysis of cyber threats ranging from Internet pranksters to violent terrorist groups

and even nation-backed cybercriminals. Readers learn about metadata and how much data they surrender to their online accounts, which are increasingly vulnerable to attacks from international hackers operating outside of national jurisdiction. Dr. Deibert moves between referencing cybercrimes such as GhostNet and Stuxnet and the masterminds behind them to the role companies like Google and Facebook play in securing user information, not only from cyber criminals but also from governments around the world. He believes private industry has too much power in policing cyberspace and that governments are trying to use these giant corporations to regulate cyber freedom and invade netizens' privacy.

Stylistically, this author is very descriptive with lengthy paragraphs that contain technical information, which some new cyber readers might find difficult to understand. His arguments are strong and have substantial supporting evidence, but are sometimes hidden within multiple layers of text. However, his broad range of evidence from different situations and locations from around the world make his argument nearly impenetrable. It would be difficult to find a hole in his arguments with the logical and convincing conclusions he presents to readers. Dr. Deibert also stresses the seriousness of cybersecurity, citing cyberwarfare and government involvement in cyberattacks against other nations as an indictment of the current state of cyberspace.

Dr. Deibert considers cybersecurity from many different perspectives and presents arguments both for and against the tightening of cybersecurity despite his personal belief in the latter. His arguments have an abundance of evidence and examples, making *Black Code* a must-read for cyber practitioners. Though his writing is at an advanced level and requires some knowledge of the cyberspace domain, readers will be captivated by his arguments' applicability and importance to their everyday lives as well as global affairs. It is an intriguing and captivating work that provides an insider perspective of the cyberspace domain with its contentious issues. The author's solutions to these global cybersecurity challenges deserve a broad audience.

Black Code: Surveillance, Privacy, and the Dark Side of the Internet

Author: Ronald J. Deibert
Publisher: Signal/McClelland & Stewart/Random House (November 19, 2013)
Paperback: 336 pages
Language: English
ISBN-10: 0771025351
ISBN-13: 978-0771025358
Price: $8.00 Paperback
$14.00 Kindle Edition

Cadet Monte Ho studies Computer Science at West Point and is a rising Cow. She is also the cadet executive officer of the Army West Point Cycling team, which is nationally ranked first by USA Cycling in Division II for 2016-2017. She is originally from Los Angeles, California and participated in an AIAD last summer, through the USC Institute for Creative Technologies in Playa Vista, involving the design of a Military Intelligence role tutorial. Upon graduation, she hopes to branch Cyber.

Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham. Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

THE CYBER DEFENSE REVIEW

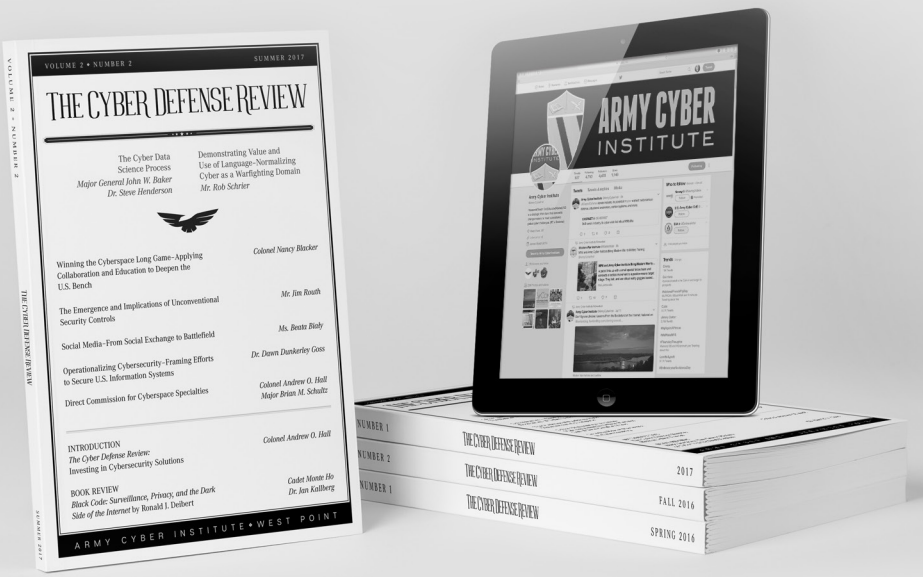
CONTINUE THE CONVERSATION ONLINE

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.