SMALL WARS JOURNAL (/)

STRATEGIC BROADENING FOR MID-CAREER CYBER LEADERS

Mad Science

Tue, 09/13/2016 - 1:25am

Strategic Broadening for Mid-Career Cyber Leaders

Brian Schultz and Blake Rhoades

Introduction

The purpose of this paper is to highlight the need for strategic broadening and policy education for mid-career Cyberspace leaders, while also providing an overview of available broadening programs that have a short-term, in-person format. As any leader progresses through the ranks, the Army often requires different skills at higher levels of responsibility; Cyberspace will not be an exception. The two programs highlighted here provide an educational jump start to mid-career leaders in the realm of strategy and policy. This paper will outline these program's requirements for eligibility, coursework, and outcomes.

Why Broaden? Why Now?

Joint doctrine defines tactics as the employment and ordered arrangement of personnel, weapons systems and support.[i] The weapons systems of cyberspace include computers, network devices, and the software to produce effects. It then follows that technical proficiency in computing, networking, system administration, and programming is required to employ the tactics of

Cyberspace, the fifth domain warfare. Proficiency in Cyberspace tactics can create a base of knowledge for leaders to understand the domain, but the Army must sow the seeds of strategic and policy education in Cyberspace leaders as they approach mid-career. As Jason Warren argues in *The Centurion Mindset and the Army's Strategic Leader Paradigm*, "…the choice of developing strategic thinkers is not a zero-sum game with tactical wherewithal."[ii]

Proficiency in tactics combined with knowledge in strategy and policy provides the best mix to handle situational complexity. Cyberspace offers a unique spin on the complexity of modern warfare. Bits move at the speed of light, the operating environment is global –but within reach, and a tactical objective can have national security impacts. This underscores the unique challenges of Cyberspace and the need for those who lead Cyberspace operations to have exposure to broadening experiences. This exposure creates positive impact on mid-career leaders in their current positions and helps raise the next generation of Cyberspace senior leaders and general officers, ensuring that they have the same strategic and policy education as their combat arms peers.

General Mark Milley, as 39th Chief of Staff of the Army, in his initial message stated, "We will do what it takes to build an agile, adaptive Army of the future."[iii] Advancements in technology will alter our future fight. Cyberspace operations of 2050 will look markedly different than Cyberspace operations of 2016, with possible advancements in robotics, artificial intelligence, and unmanned vehicles. Emphasizing and refining existing strategic broadening programs will assuredly impact tomorrow's mid-career leaders. We should keep in mind that among the Cadets and Lieutenants of today are the future Generals that will shape the Army and Cyberspace operations of 2050. Ensuring that we refine, strengthen, and adapt our mid-career broadening programs to better educate tomorrow's mid-career leaders has become more important than ever.

Longer-term graduate schooling or joint assignments can provide broadening experiences, but may not efficiently fit into a leader's career path. With advancements in technology and telecommunications, professionals across the military and industry can increasingly achieve broadening experiences through part-time and online education; however these outlets often lack an opportunity to network with peers and more senior professionals. Short, in-person, seminars may provide an optimal middle-road for a number of leaders. The remainder of this paper focuses on highlighting two short-term programs available to mid-career Cyberspace leaders that provide strategic and policy education while maintaining those leaders in their current assignments. This approach benefits the leader and the Army, but does not require a change of station and all the accompanying administrative costs.

SBS Program at Indiana University

Overview

Under the direction of General Odierno, while serving as the 38th Chief of Staff of the Army, HQDA implemented the Strategic Broadening Seminar (SBS) Program.[iv] SBS serves as an umbrella program under which universities host three to five week long seminars. The SBS Program has educated mid-career Army Leaders since 2014 at locations as diverse as the Defense Academy of

the United Kingdom, and the Interdisciplinary Center in Israel, but also as local as the University of North Carolina, University of Louisville, University of California Berkeley, University of Kansas, and Indiana University (IU).[v] IU's inaugural seminar in 2016 was the first to offer a Cyberspace-themed curriculum and capstone project. The remainder of this section provides a broad outline of this seminar, details the seminar capstone, and provides a recommendation on who should participate in this Cyberspace-themed strategy seminar in the years to come.

The first seminar at IU concluded in June 2016 and graduated 23 Army leaders with backgrounds including Special Operations, Military Intelligence, Medical Corps, Logistics, Signal Corps, and Cyber. Ranks ranged from Sergeant First Class to Major. The seminar was designed as an immersive three-week experience which allows leaders to break from everyday leadership and administrative tasks to focus on complex strategic security issues in a collegiate environment. IU is uniquely positioned to host a seminar focused on Cyberspace strategy given its blend of Cybersecurity and national security faculty and resources. IU also greatly benefitted from its partnership with the Institute for Defense and Business (IDB). IDB administers the SBS program at both the University of North Carolina and IU under the title of Strategic Studies Fellows Program. With facility space and faculty provided by the host university, IDB enriches the academic seminar by providing the opportunity to meet with local industry and strategic leaders forming a cohesive experience that touches government, academia, and industry.

IU's seminar included an expansive look at several Cyberspace strategy areas, to include: Internet Governance, Domestic Cyberspace Law, Information Security, and Risk Mitigation implementation. Within these themes students grappled with unique issues that have strategic impact in Cyberspace. For instance, Internet Governance is regulated in a distributed multi-stakeholder format, the domain has a significant attribution problem, and technology is making data collection and analysis on private civilians easier than ever. Figure 1 illustrates just one example scenario which groups of student picked a policy solution and defended their choice in front or their peers.[vi] This example scenario speaks to the level at which students interacted with Cyberspace issues.

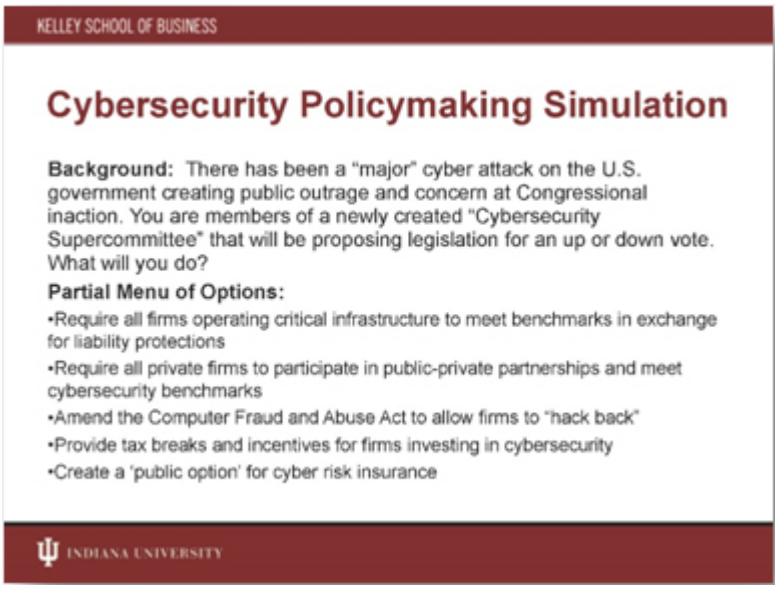

Figure 1. Example Scenario from SBS Program

IU's network of alumni, faculty, and relationships in the national security realm allowed the inaugural program to include lectures with former Ambassador Lee Feinstein and former Congressman Lee Hamilton, vice-chair of the 9/11 Commission and co-chair of the Iraq Study Group. Students also spent an evening with former commander of USNORTHCOM, GEN (Ret) Victor Renuart and spent a day with Dr. Peter Feaver from Duke University, discussing National Security Strategy (NSS) and National Military Strategy. Feaver's previous experience in the National Security Council provided great insight on why we publish the NSS and how the NSS should trickle down to the strategies laid out in subordinate departments and agencies.

The seminar weaved through lessons on understanding emerging trends and global flashpoints with topics including: the expansion of global terrorist networks, the collapse of political order in the Middle East, and the maritime dispute in the South China Sea. In the years to come, the seminar could better incorporate how Cyberspace impacts emerging trends and global flashpoints, a recommendation that has already been offered to IU faculty. For instance, lectures focused on ISIL or Russian actions in Eastern Europe prove useful; however, faculty could reinforce the seminar's theme by drawing out how these actors have used Cyberspace to recruit, spread ideology, and even deny command and control to their adversaries.

Other elements of the seminar focused on international relations. For example, students received an interesting lecture on the role nuclear deterrence has played in Pakistan-India relations. While this subject matter does not directly link to Cyberspace strategy, it challenges leaders to think about deterrence in general and the role traditional deterrence may play in the future of Cyberspace. Deterrence options may include sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures.[vii] Some deterrence options appear effective when levied against nation-state actors[viii]; however the ubiquity of Cyberspace weapons and difficulty of attribution in Cyberspace does not guarantee that our traditional deterrence options will always success against a variety of threats –state or non-state– in the future.

The Capstone Project

The capstone project challenged leaders to develop a strategic response plan to a cyber-attack in Indiana. Students delivered a short paper and presentation which highlighted short-term and long-term response actions from every echelon of government from local to federal. Students learned that domestic laws governing cyber-crime can often be outdated or ambiguous, and that international laws and norms can often completely lack consideration for cyber-attacks. For instance, the North Atlantic Treaty expressly states the right to collective defense in the face of "armed conflict" but lacks language accounting for cyber warfare.[ix] In this vain, many student groups made recommendations to change existing international treaties –or to create new ones altogether.

The capstone scenario correctly captured the complexity that an escalation of cyber warfare could have. Students had to address the erosion of the American sense of security while at home in their own communities. Students also addressed how widespread Cyberspace aggressions could create a global financial calamity. In the end, students briefed their recommendations to a diverse panel

that included Dr. Scott Schakelford of IU, BG Maria Barrett of Army Cyber Command, COL Chris Croft of the Combined Arms Center, MG (Ret) Jim Hodge of the Institute for Defense & Business, and the Indiana National Guard.

Who Should Attend an SBS Seminar?

The broadening opportunity provided by an SBS seminar would serve useful for any mid-career leader. IU's Cyberspace theme is very much the vehicle in which students learn about US National Security Policy and leaders do not need any prior experience in the domain. Acceptance into any SBS Program requires a letter of recommendation from a Brigade Commander, Colonel Supervisor, or GS-15 equivalent. Particular programs under the SBS umbrella may require a Bachelor's degree. [x] Human Resources Command releases a new MILPER message every year for the SBS Programs that will take place during the upcoming fiscal year. Applicants should pay close attention to this message to determine their eligibility.

MPF Military-Business Cybersecurity Fellowship

Overview

Alternatively, the Madison Policy Forum (MPF) provides another broadening option available to mid-career leaders. MPF is a privately funded, philanthropic initiative that seeks to solve designated societal and national security issues through a variety of programs. MPF's Military-Business Cybersecurity Fellowship aims to, as the title indicates, establish relationships between cybersecurity professionals in military, public, and private sectors, with the hope that these individuals continue to collaborate on Cyberspace crises throughout their careers. The fellowship leans toward a public policy focus, but draws on the informed experience and knowledge of its technically adept fellows.

Public policy is essentially the art of decision-making and should be a core competency for any Army leader. As officers progress in rank, it often becomes necessary for them to interact with organizations outside of the Chain of Command and, perhaps, outside of the Army or government. This fellowship uses the idea of cross sector relationships to help officers better understand a *holistic* approach to cybersecurity by better familiarizing fellows with the issues and roles of a variety of organizations. Such experiences will undoubtedly help mid-career officers to better understand the Army's role in secure our nation in cyberspace, while simultaneously introducing them to outside experiences and resources.

MPF's Cybersecurity fellows meet in Manhattan on a monthly basis throughout the year to learn more about the unique Cyberspace problems faced by each sector: military, private, and public. Meeting venues for the 2016 fellowship included: Virtu Financial's Headquarters in New York City, Fordham Law School in New York City, and the Army Cyber Institute in West Point, NY. At each event, fellows take the opportunity to discuss Cyberspace problems in their respective sector and often share lessons learned and best practices with the group.

The participants often discuss strategic Cybersecurity challenges that are omnipresent throughout all sectors, and are given the opportunity to conduct cross-sector academic research against these problem-sets. At the conclusion of the fellowship, MPF fellows deliver an academic, peer-reviewed paper for publication.

After fellowship completion, alumni continue to remain in contact and are often called upon to assist current fellows, to attend reunion events, and to speak at fellowship luncheons or other events. In many cases, alumni have used the MPF email distro to disseminate other professional development opportunities. To date, distinguished alumni from the fellowship include representatives from the banking industry, state level Cybersecurity agencies, the private Cybersecurity sector, the Federal Bureau of Investigation, the State Department, the Treasury Department, the Commerce Department, along with several leaders from the Cyber Mission Force.

Given the diversity of the alumni and the frequency of interaction, the program has provided a strong opportunity to create a network of competent cybersecurity professionals. In an era where information-sharing and cross-sector communication has become essential to success in Cyberspace, the value of these relationships is tremendous for the U.S. Army and the Cyber Mission Force.

Who Should Attend MPF's Cybersecurity Fellowship?

Mid-career officers and warrant officers currently assigned or will be assigned to the Cyber Mission Force are particularly well suited for this fellowship. The MPF selection process is highly competitive and seeks highly successful professionals to attend the cohort every year. Candidates are evaluated based on their work experience, academic background, and writing abilities. Thus, leaders with strong academic backgrounds, excellent recommendations from previous commanders, and outstanding writing skills are best suited for the program.

Conclusion

In the Cyberspace domain, mid-career leaders with an interest in national strategy, policy, and international relations should strive for a breadth of educational experiences. An SBS seminar or an MPF fellowship are two options available to leaders. Such programs are helpful methods that enable broadening for Cyberspace leaders with short programs that do not require a change of station or additional service obligation.

Not all broadening opportunities fit the short-program mold provided by an SBS seminar or MPF fellowship. Other options may attract Cyberspace leaders. Some alternatives require very little travel, while others could require a permanent change of station for a longer assignment in a broadening billet. Broadening assignments available through Human Resources Command can provide a fully immersive experience and Cyberspace leaders of the future should engage branch representatives for more information on joint or non-traditional billets.

Cyberspace leaders can also broaden their horizons through membership in professional or technical organizations. Seeking out term membership in the Council of Foreign Relations or becoming an at-large member of the Internet Corporation for Assigned Names and Numbers has the

potential to educate leaders about international and Internet policies. In addition, many universities offer online certificates in strategic planning through their respective business or graduate schools. Along with these other opportunities, broadening experiences provided in short-term programs like an SBS seminar or the Madison Policy Fellowship can provide invaluable education while maintaining leaders in their current assignments and still providing an opportunity to interface with peers and senior professionals in a face-to-face manner.

Any of these options has the potential to educate mid-career leaders on strategy and policy; ultimately aiding the leader and the Army in the process. In her graduation speech to students at the IU seminar, BG Barrett explained that broadening your mind is like doing an exercise you have not done in a while.[xi] Unused muscles become sore after a good workout, but the diversity in exercise is necessary for overall health. In the same way, exposure to a mix of tactics, strategy, and policy furthers a Cyberspace leader's capacity to handle situational complexity in their current and future positions.

End Notes

[i] U.S. Department of Defense. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms. 89-235. Accessed August 2, 2016. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[ii] Warren, Jason W. "The Centurion Mindset and the Army's Strategic Leader Paradigm," *Parameters* 45, no.3, 27-38. Accessed June 18, 2016. https://www.strategicstudiesinstitute.army.mil/pubs/parameters/issues/Autumn_2015/6_Warren.pdf.

[iii] "Initial Message to the Army." Letter from Mark A. Milley. Accessed July 29, 2016. https://www.army.mil/e2/rv5_downloads/leaders/csa/Initial_Message_39th_CSA.pdf.

[iv] Vergun, David. "Two New Programs Broaden Opportunities for Eligible Soldiers." www.army.mil (http://www.army.mil). February 20, 2014. Accessed June 18, 2016. https://www.army.mil/article/120518/Two_new_programs_broaden_opportunites_for_eligible_Soldiers.

[v] *MILPER Message Number 15-219*. July 15, 2015.

[vi] Shackelford, Scott. "Global Cybersecurity Governance." Lecture, SBS Program, Indiana University, Bloomington.

[vii] Gertz, Bill. "Obama Considering Range of Options in Response to OPM Hack." Washington Free Beacon. June 17, 2015. Accessed July 29, 2016. http://freebeacon.com/national-security/obama-considering-range-of-options-in-response-to-opm-hack/.

[viii] FireEye, Inc. ISight Intelligence "Redline Drawn: China Recalculates Its Use of Cyber Espionage." News release, June 2016. Accessed June 29, 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[ix] "The North Atlantic Treaty." NATO. Accessed June 01, 2016. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[x] *MILPER Message Number 15-219*. July 15, 2015.

[xi] Barrett, Maria. “Graduation Speech.” Speech, SBS Program, Indiana University, Bloomington, June 4, 2016.

Categories: Mad Scientist (/taxonomy/term/306)

About the Author(s)

(/author/blake-rhoades)

Blake Rhoades (/author/blake-rhoades)

CPT Blake Rhoades is a member of the Army Cyber Institute and an Instructor of International Relations in the Department of Social Sciences. From 2012-2013, he was the company commander of the Army's first Cyber National Mission Team at the 780th MI Brigade in Ft. Meade, MD, and has deployed twice as a signals intelligence platoon leader in support of Operation Iraqi Freedom. He holds an M.S. in Information Security Policy and Management from Carnegie Mellon University and a B.A. (Political Science) from the University of Alabama. He was recently selected as a 2016 Madison Policy Forum cybersecurity fellow. His research interests include Public policy, cyber, and national security.

(/author/brian-schultz)

Brian Schultz (/author/brian-schultz)

CPT Brian Schultz is a member of the Army Cyber Institute and an Instructor of Information Technology in the Department of Electrical Engineering and Computer Science at West Point. From 2014-2015, he served as the Chief of Cybersecurity for the 8th Sustainment Command in Ft. Shafter, HI, 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. (Communication) from Millikin University. He is currently studying Computer Science at DePaul University and his research interests include talent development and systems exploitation.

-