Strategic Broadening for Mid-Career Cyber Leaders

BRIAN SCHULTZ AND BLAKE RHOADES

Why Broaden? Why Now?

Proficiency in the technical aspects of computing, networking, and Cyberspace is required to understand, and eventually master, the tactics of what has been called the "fifth domain". While proficiency in Cyberspace tactics forms a base of knowledge to understand capabilities and limitations, 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"[1].

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 also helps raise the next generation of Cyberspace general officers and their staffs, ensuring that they have the same strategic and policy education as their combat arms peers.

This paper provides a broad outline of two short-programs available to mid-career Cyberspace leaders that provide strategic and policy education while maintaining those leaders in their current assignments. This aids the leader attempting to ingest strategic thought and policy considerations back into their current work role and 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 Chief of Staff of the Army, HQDA implemented the Strategic Broadening Seminar (SBS) Program.[2] SBS serves as an umbrella program under which universities host three to five week long strategic broadening seminars. The SBS Program has educated mid-career Army Leaders since 2014 at locations as diverse as the Defense Academy of the United Kingdom, University of North Carolina, University of Louisville, the Interdisciplinary Center in Israel, University of California Berkeley, University of Kansas, and Indiana University (IU).[3] IU's inaugural seminar in 2016 was the first to offer a Cyberspace-themed curriculum and capstone project. 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, and Signal Corps. 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

[1] Warren, Jason W. "The Centurion Mindset and the Army's Strategic Leader Paradigm," *Parameters* 45.3 (Autumn 2015): 2. Web.

[2] Vergun, David. "Two New Programs Broaden Opportunities for Eligible Soldiers." www.army.mil. US Army, 20 Feb. Web. 18 June 2016.

[3] U.S. Army. HRC *MILPER Message Number 15-219*. N.p.: n.p., 2015. Print.

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.

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. This example scenario speaks to the level at which students interacted with Cyberspace issues.

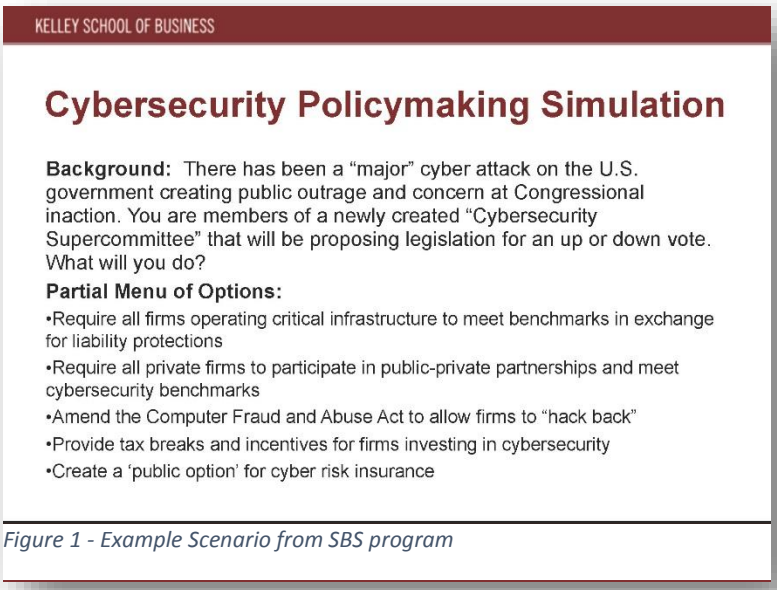

Figure 1 - Example Scenario from SBS program

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, this sort of in depth

look at a particular global flashpoint almost begs the question, what does deterrence 'look like' in Cyberspace. Publically, the US boasts a suite of responsive actions including sanctions, indictments, cyber retaliatory options, and even the threat of kinetic measures.[4] A recent downturn in Chinese Cyberspace activity directed toward the US appears to have resulted from US indictments and the threat of economic sanctions[5]; however, these deterrence options remain largely untested and do not necessarily guarantee success against a variety of threats 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 from local, to state, to federal, and even prescribed recommendations for NATO. 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.[6] 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 and cause a run on physical currency, as an overwhelming portion of the world's wealth only exists in electronic form.

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. Consider this: every commissioning source in the Army teaches leadership through the lens of light Infantry tactics. Cadets and Candidates lead peers in staging ambushes and assaulting bunkers, but only a minority of these soon-to-be officers actually serve in light infantry units; however, these drills are useful in developing basic leadership skills. Similarly, IU's Cyberspace theme is very much the vehicle in which students learn about US National Security Policy. Only a minority of the leaders educated in the seminar will serve in Cyberspace units; however the experience will prove useful in developing strategic thinking skills for any leader.

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

[4] Gertz, Bill. "Obama Considering Range of Options in Response to OPM Hack." *Washington Free Beacon*. Washington Free Beacon, 17 June 2015. Web. 19 June 2016.

[5] FireEye, Inc. *Redline Drawn: China Recalculates Its Use of Cyber Espionage*. Rep. Milpitas, CA: FireEye, 2016. Web. 29 June 2016.

[6] "The North Atlantic Treaty." *NATO*. North Atlantic Treaty Organization, 21 Mar. 2106. Web. 1 June 2016.

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.

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.

Who should attend MPF's Cybersecurity Fellowship?

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 have become essential to success in Cyberspace, the value of these relationships is tremendous for the U.S. Army and the Cyber Mission Force.

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.

Conclusions

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. Options that require very little travel or 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 university offer online certificates in strategic planning through their respective business or graduate schools. Cyberspace leaders can also submit original papers or presentations to a variety of academic or trade publications to include the Cyber Defense Review, the Small Wars Journal, or Association for Computing Machinery.

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. As BG Barrett stated in her graduation speech to students at the IU seminar, “Broadening your mind is like doing an exercise you haven’t done in a while.” 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 leaders’ capacity to handle situational complexity in their current and future positions.