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.

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.

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

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.