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.