CENTER for STRATEGIC LEADERSHIP CSL

Issue Paper

Center for Strategic Leadership, U.S. Army War College

February 2010
Volume 1-10

War is War?

The utility of cyberspace operations in the contemporary operational environment

Workshop Initial Impressions

Dennis Murphy, United States Army War College

History teaches us that the character of each individual war is always different and most certainly will change, but the enduring nature of war as a human endeavor will remain largely unchanged.

—General James N. Mattis

The United States Army War College in partnership with The SecDev Group conducted a workshop examining cyberspace operations from the warfighter's perspective. The workshop was held 26–28 January 2010 at the Collins Center for Strategic Leadership, U.S. Army War College, Carlisle Barracks, Pennsylvania.

BACKGROUND

The U.S. Department of Defense (DoD) defines cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace." Cyberspace emerged as a national-level concern through several recent events of geo-strategic significance. Estonian infrastructure was attacked in the spring of 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against Georgia. It is plausible that such complex excursions may become the norm in future warfare among nation-states having the capabilities to conduct them. Much has been written about the issues of cyberspace at the national strategic level: lack of attribution and the applicability of the law of armed conflict and of international treaties, and the determination of criminality vice acts of war. But the current body of knowledge does not inform us about how the concept of cyberspace operations impacts and will be adapted by warfighting commanders in the contemporary and future operational environments. The workshop examined this issue and used the Russia-Georgia case study to draw lessons to apply to current and future warfare.

The workshop centered on three challenges. The first challenge considered conducting a campaign where cyberspace is contested/constrained and the impact on U.S. warfighting concepts and practices. The second challenge considered the strategic frame from the perspective of integrating cyberspace operations into the overall campaign and the applicability of existing joint operating concepts, capabilities, relationships, and authorities to the cyberspace domain. The final challenge considered situational understanding in terms of how cyberspace operations fit within the warfighting commander's mission set across the full spectrum of conflict. It specifically considered how to gain situational understanding as input to planning and executing joint operations.

WORKSHOP DESIGN

The workshop brought together an international audience of military, national security community, and intelligence community leaders as well as experts from academia. It was conducted over the course of three days and began with a plenary session, a keynote presentation, and a dinner address to set the stage for the subsequent presentations and discussions. Day

Professor Dennis M. Murphy is the Director of the Information in Warfare Group, part of the Science and Technology Divison of the Center for Strategic Leadership, United States Army War College.

two included additional plenary presentations to establish a foundation of understanding followed by breakout groups that addressed the key issues involved in order to satisfy workshop objectives. Day three was devoted to briefing the recommendations, observations, and insights gained from the breakout groups to the plenary group and to blue ribbon senior panels in Washington and Ottawa.

The plenary sessions defined and analyzed the scope, nature, and impact of cyberspace operations employed in conjunction with other actions by parties during the Russia-Georgia conflict of 2008. Specifically, these sessions sought to better understand the assumptions, intent, and the strategic frame (or lack thereof) employed by military actors in the conflict. These sessions also provided an opportunity to debate a key question: has the recognition of cyberspace operations as a capability within a new warfighting domain changed the nature of warfare...or is it more simply another capability to be integrated into an age-old system and process of planning and execution? (Thus the title: "War is War?") Beyond the case study, guest speakers provided uniquely different perspectives regarding cyberspace operations, from its parallel applicability to current military paradigms within geographic combatant commands, to cautions regarding the application of resources against a domain that may not be decisive by its very nature. Breakout groups drew lessons from the case study and from the guest speakers for application to questions of current and future conflict.

WHY THIS WORKSHOP AND WHY NOW

How does cyberspace impact the way we conduct warfare today? Certainly the United States is already conducting cyberspace operations, and has been for some time. And obviously so are our competitors, adversaries, and potential enemies. So is this concept evolutionary or revolutionary, or are we simply now providing more focus given our dependence on cyberspace to both plan and conduct operations? There are a number of factors that point to the increasing relevance of cyberspace as both an enabler and potential vulnerability to the warfighter.

Beyond the nation-state cases of Estonia and the Russia-Georgia conflict, cyberspace plays a critical role across the spectrum of joint military operations. Consider how cyberspace operations impacted U.S. Southern Command's humanitarian response efforts in Haiti, where real time images and reports focused on both positive and negative aspects of the relief effort; U.S Africa Command's theater security engagement, where even with low internet penetration percentages across the continent, Africa has seen an increase in internet use of over 1000% from 2000 to 2009; and USCENTCOM's counterinsurgency efforts, where adversaries use cyberspace as the dominant domain to propagate information as a strategic weapon while coalition forces increasingly fight back by providing contextual news on social networking sites and forensic information within cyberspace to proactively counter expected enemy propaganda.

Recognizing the current and future importance of the cyber domain and cyberspace operations within it, the DoD has moved forward on a number of fronts. Cyberspace is prominently emphasized in the recently released 2010 Quadrennial Defense Review. The DoD "seeks strategic, operational, and tactical cyberspace capabilities that provide: U.S. freedom of action in cyberspace, to include freedom from unwanted intrusions and the ability to deny an adversary's freedom of action in cyberspace; global situational awareness of cyberspace and; the ability to provide warfighting effects within and through the cyberspace domain that are synergistic with effects within other domains" (Quadrennial Roles and Missions Review, 2009). The establishment of the nascent U.S. Cyber Command as a sub-unified combatant command sends a loud message regarding the importance of cyberspace to the warfighter.

While the relevance of cyberspace operations is evident by these documents and actions, the specific challenges, issues, and solutions to fighting in cyberspace while synchronizing land, maritime, air, and space operations remain emergent and subject to discussion. These subjects were presented in the plenary sessions and subsequently discussed in detail within the breakout groups. Three themes emerged: the need for common understanding of terminology and capability, the will to employ cyberspace operations at the speeds needed to employ them, and the need to "grow" cyberspace warriors at all levels.

COMMON UNDERSTANDING

Participants generally felt that current DoD cyberspace definitions were both programmatic (which made them limiting) and difficult to understand. For instance, "cyberspace" is defined, while other domains such as land and sea are not. Cyberspace operations are also defined: "The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities

to operate and defend the Global Information Grid." On the other hand, there is no definition of "land operations" or "maritime operations," since these are generally assumed to be military operations occurring within these respective domains. Consequently, participants wondered why cyberspace operations are not simply "operations conducted in cyberspace." While a case could be made regarding the unique manmade and global nature of the domain itself justifying a definition, the current programmatic definition along with the above-mentioned definition of cyberspace operations complicates an understanding of the concept for warfighters. In a similar vein, participants discussed emergent joint cyberspace doctrine and how it should be crafted in light of current joint doctrine. Specifically "joint functions" and "design elements" such as "synchronization," "maneuver," "fires," and "effects" in cyberspace operations were considered. There was strong consensus among participants that current joint functions and terminology apply to the cyberspace domain and should be used when referring to cyberspace operations.

However, there was a note of caution that used the concept of "maneuver" as an example. Participants recommended direct application of the lexicon "maneuver" (which involves achieving positional advantage), but strongly noted that the nature of time, space, velocity, and volume of engagement in cyberspace must both color and inform the application of maneuver within that domain as opposed to the traditional domains. In contrast to the call for adoption of current joint functions and operational design lexicon, there was consensus that the terms "superiority" and "dominance," as applied to cyberspace, were generally unachievable given the variety of actors who impact the domain. Alternatively, effective management of cyberspace must become the accepted norm, reflecting both proactive consideration and "proactively reactive" response. Finally, the concepts of connectivity, content, and cognition were considered. It was felt that U.S. warfighters focused on the "connectivity" aspects of cyberspace (the "wires" and infrastructure) as opposed to the content and cognition dimensions. On the other hand, our adversaries consider connectivity principally as a means to exploit content and cognition. The United States needs to adopt a more holistic consideration of all three dimensions in that light.

WILL vs. VELOCITY

Participants on more than one occasion questioned the unclassified nature of the workshop as potentially limiting to a full consideration of the challenges presented. On the other hand, it allowed a discussion of the very nature of cyberspace as a warfighting domain and those same security classification issues as limiting the warfighter's ability to understand and exploit cyberspace. Cyberspace, it was noted, is not purely confined to military operations and systems. In fact, cyberspace operations are perhaps the epitome of what is currently referred to as "JIIM" (Joint, Interagency, Intergovernmental, Multinational) operations; that is, all current and future operations will be conducted in an environment that inherently involves more than military capabilities and more than U.S. forces and actors. Thus, security classification must be considered with this in mind. Sharing information with allies and partners will ensure the avoidance of "cyberspace fratricide" and expose gaps, seams, and overlaps as well as second and third order effects of planned cyberspace operations. Sharing and exchanging information with industry will allow the military to understand procedures for nimbleness of action and reaction in cyberspace, where industry adapts more quickly. Consequently, a consideration of using classification policy to first determine what can remain unclassified vis-à-vis cyberspace – vice a tendency to classify first and then declassify after an exhaustingly long process – might go a long way toward demystifying and enabling cyberspace operations.

On the other hand, participants acknowledged the Clauswitzian tenet that war is politics by other means. Military operations in cyberspace require the will of civilian leaders who must acknowledge requirements and provide authorities that support rapid actions in the cyberspace domain. While this may involve a tiered approach to rules of engagement, the speed-of-light nature of the domain certainly requires, at some level, decentralized decisions and actions with commensurate oversight and guidance.

GROWING CYBER WARRIORS

Participants noted often the need for specific focus on people, processes, and organizations as they apply to cyberspace and cyberspace operations. While perhaps cliché, they recognized that, given the dependency of military operations on computers and the Internet, all warriors are cyber warriors. Consequently, education and training are required not only for technical experts but for all military members at all levels of professional military education. This may

be particularly critical for senior leaders who are digital immigrants but who must advocate and obtain resources for this vital, though nascent, warfighting function. The importance of education was further emphasized by a member of the blue ribbon panel who noted that "we are not network enabled; we are network dependent." The type of and need for this recommended education may be further defined by the military organizations that emerge in support of combatant command cyberspace operations.

Two schools of thought dominated breakout group discussion in this regard. First, there was a position that advocated that U.S. Cyber Command assume a Special Operations Command-like structure. This would engender global situational understanding, support the specialized but low-density skills needed to practice cyberspace operations, and provide a more centralized capability to understand adversaries and their decision cycles in this regard. Another position advocated a cyber component command directly subordinate to the geographic combatant command (similar to component commands provided in other domains). The Navy's Information Warfare Group, which has a global view but is in direct support of a regional command, was offered as a potential model. The former approach provides centralized control of specialized forces but may require prioritization of limited assets; the latter, direct control of forces in theater and an expectation of more immediate response to regional requirements.

Finally, it was noted that current intelligence support to cyberspace is grossly lacking in numbers, education, and organizational culture. Growing an intelligence capability to support this domain is a critical component of future success.

CONCLUSION

Cyberspace and cyberspace operations are both important to today's military operational environment and have the potential to become critical to operational success within the future environment. The United States has recognized this and taken initial steps to establish policies, processes, and doctrine to operate within cyberspace. But the specific near-term decisions regarding cyberspace are critical to efficiently and effectively achieve success in integrated joint military operations. The "War is War?" workshop is one step toward recognizing that need and moving to address it. A comprehensive workshop report will be completed by the Center for Strategic Leadership and the SecDev Group in cooperation with workshop participants with a target publication date of summer, 2010.

****

This and other CSL publications may be accessed for free through the USAWC/CSL web site at: http://www.csl.army.mil.

****

WAR IS WAR?

U.S. ARMY WAR COLLEGE
Center for Strategic Leadership
650 Wright Avenue
Carlisle, PA 17103-5049

OFFICIAL BUSINESS