War is War

A workshop on the strategic utility of cyberspace operations in the contemporary operational environment

Dennis Murphy, U.S. Army War College and Rafal Rohozinski, The SecDev Group

"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 will conduct a workshop examining cyberspace operations from the warfighter's perspective. The workshop will be 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 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 allegedly again conducted cyber attacks this time in a coordinated and synchronized kinetic and non-kinetic campaign against Georgia. It is plausible that this may become the norm in future warfare among those nation-states having the capabilities to conduct such complex excursions. Much has been written about the issues of cyberspace at the national strategic level: lack of attribution; applicability to the law of armed conflict and international treaties; determination of criminality vice act of war. But the body of knowledge does not inform us about how this concept of cyberspace operations impacts and will be adapted by warfighting commanders in the contemporary and future operational environment. The workshop seeks to examine this issue and use the Georgia-Russia case study to draw lessons to apply to current and future warfare.

The workshop will center on three themes. The first theme considers the strategic frame from the perspective of defining cyberspace as a domain of military operations including a consideration of what defines "maneuver" in cyberspace. The second will consider situational understanding in terms of how cyberspace operations fit within the warfighting commander's mission set across the full spectrum of conflict. It will specifically consider how to gain situational understanding as input to planning and executing joint operations. The final theme considers cyberspace "fires," that is the toolset such as authorities and rules of engagement that determine strategic utility and tactical applicability.

OVERALL WORKSHOP OBJECTIVE

The objective of the workshop is to examine the strategic utility of cyberspace operations in the existing contemporary and future operational environment from the perspective of the warfighter.

WORKSHOP DESIGN

The workshop will bring together an international audience of military, national security community and intelligence community leaders as well as experts from academia. It will be conducted over the course of three days and will begin with a plenary session and a dinner and keynote speech to set the stage for the subsequent presentations and discussions. Day two will include additional plenary presentations to establish a foundation of understanding followed by breakout groups which will address the key issues involved in order to satisfy workshop objectives. Day three will be devoted to briefing the recommendations, observations and insights gained from the breakout groups to the plenary group.

PROPOSED PLENARY SESSION AND BREAKOUT GROUP TOPICS

1. The plenary sessions will define and analyze the scope, nature and impact of cyberspace operations employed in conjunction with other actions by parties to the conflict during the Georgia-Russia conflict of 2008. Specifically, these sessions will seek to better understand the assumptions, intent, and the strategic frame (or lack thereof) employed by military actors in the conflict. The plenary also provides 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?

2. Breakout groups look to draw lessons from the case study for application to current and future conflict. Three groups will consider: operating in a constrained cyberspace domain; integrating cyberspace operations into the overarching campaign plan across the spectrum of conflict; and, achieving situational understanding to enable effective cyberspace operations.

WORKSHOP DELIVERABLES

A report reviewing the key issues, discussions, findings and recommendations of the workshop will published by the Center for Strategic Leadership and The SecDev Group.

TENTATIVE AGENDA

Tuesday, 26 January 2010 – The Collins Center

1330–1430 Arrive and Register
1430–1700 Plenary Session, Setting the Stage (Normandy Room, 3rd Floor)
1800–2100 Cocktails and Dinner w/Keynote Speaker (Letort View Community Center)

Wednesday, 27 January 2010 – The Collins Center

0830–1030 Plenary Session, Setting the Stage (Normandy Room, 3rd Floor)
1030–1200 Small Group Discussion (Team Rooms, 2nd Floor)
1200–1300 Lunch (Ardennes Room)
1300–1700 Small Group Discussions (Team Rooms, 2nd Floor)
1700–1800 Briefing Development (Team Rooms, 2nd Floor)
Dinner on your own

Thursday, 28 January 2010 – The Collins Center

0800–0900 Briefing Development (continued) (Team Rooms, 2nd Floor)
0900–1200 Panel Briefs and Discussion (Normandy Room, 3rd Floor)
1200   Wrap-up and Adjourn (Normandy Room, 3rd Floor)

CONTACT INFORMATION

For additional information regarding this event please contact Professor Dennis Murphy at 717-245-3937, or Mr. Jerry Johnson at 717-245-3392. Email: dennis.murphy@us.army.mil or jerry.dwayne.johnson@us.army.mil.