CYBERSPACE OPERATIONS

What Senior Leaders Need to Know About Cyberspace

William Waddell

David Smith, James Shufelt, Jeffrey Caton

CSL Study 1-11
March 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Center for Strategic Leadership,650 Wright Avenue,Carlisle,PA,17013-5049**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**35**	

The United States Army War College

The U.S. Army War College prepares selected military, civilian, and international leaders for the responsibilities of strategic leadership in a joint, interagency, intergovernmental and multinational environment. The U.S. Army War College:

- Educates select military, civilian, and international leaders
- Supports worldwide practitioners
- Conducts research, and publishes to inform thought
- Supports the Army's strategic communication efforts
- Provides comprehensive well-being education and support
- Graduates more than 300 SLC JPME Phase I-certified, and 340 JPME II-certified leaders each year

The Center for Strategic Leadership

The Center for Strategic Leadership serves as a high-technology senior leader experiential education center which:

- Educates selected current and future military and civilian senior leaders, with emphasis on land power in a JIIM environment at the operational and strategic levels of war
- Supports the intellectual endeavors of key Army operational and force generating organizations and the broader national security community
- Conducts and hosts research activities and publishes on relevant strategic subjects
- Assists with Army strategic communication efforts

Key to the capability of the CSL is our ability to deal with issues using the project team concept. The CSL has the ability to pull together regional or functional teams which, in addition to the core CSL personnel (subject matter, computer, and model expertise), could include members of the Strategic Studies Institute, contractors, and other academic institutions. This project team concept allows us to develop a team, complete a tasking, and then change the team based upon new requirements.

CYBERSPACE OPERATIONS

What Senior Leaders Need to Know About Cyberspace


Prudens
Futuri

CYBERSPACE OPERATIONS

What Senior Leaders Need to Know About Cyberspace

A workshop to explore how academia should prepare future senior leaders for emerging Cyberspace challenges.

Mr. William Waddell

with

Professor David Smith, Mr. James Shufelt, and Colonel Jeffrey Caton

CENTER for STRATEGIC LEADERSHIP

CSL

U.S. ARMY WAR COLLEGE

CSL Study 1-11
Carlisle, PA
March 2011

Acknowledgements

This report documents the procedures of the Cyberspace Operations Workshop, conducted June 15-17 2010, by the Center for Strategic Leadership at the Collins Center, United States Army War College. Thanks go to the following personnel for their assistance in making this workshop a success:

Ms Wendy LeBlanc – Workshop Administration

Professor Cindy Ayers – Guest Speaker Coordination

Administrative Support Team: Mr. Ken Chrosniak, Colonel Mike Fulford, Colonel Frank Rebholz, Colonel W. David Mead, Colonel Damon Igou, Colonel Kimball Hubbert, and Lieutenant Colonel Robert Farneth

Mr. Romaine Leake – Information Technology Support

This and other CSL publications are available on line at:

http://www.csl.army.mil

U.S. ARMY WAR COLLEGE

CARLISLE BARRACKS, PENNSYLVANIA 17013

Contents


Prudens
Futuri

CYBERSPACE OPERATIONS WORKSHOP

Workshop Report

…the cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country…
—President Barack Obama, May 29, 2009

The Federal Government, in partnership with educators and industry, should conduct a national cyber security public awareness and education (program).
—*Cyberspace Policy Review,* 2009

The United States is dependent on computer networks for rapid sharing of information and the operation of critical infrastructure. The daily lives of Americans and many other global cultures rely on increasingly vulnerable networks for electric power, finance, education, and a host of other critical but often taken-for-granted services. Cyberspace, in its working definition is ubiquitous across government and private industry, from national defense to small private enterprises connecting all aspects of life unlike any other medium in human history. The Internet, as it was originally conceived and evolved, gave little priority to security. Therefore, its vulnerabilities grow as more critical government and private organizations increasingly depend upon its availability to conduct day-to-day operations. In the military, concepts such as Information Operations and Network Centric Warfare rely on complex information systems that utilize global computer networks. Until 2009, most requirements and decisions on network security and capability were made by communications experts, especially in the military. However, as dependence on this vulnerable network increases, commanders must be directly involved because of the great operational impact of network failure or degradation. There is concern that many senior leaders are being thrust into an area for which they are poorly equipped due to lack of cyberspace education or experience. As cyberspace operations are now fully embedded in military operations, it is imperative that academic institutions provide cyberspace education opportunities for our future commanders as well as government and private sector leaders.

Based on this new educational requirement, the Cyberspace Operations Group of the Center for Strategic Leadership, U.S. Army War College, conducted a

three-day workshop to explore the cyberspace issues that should be addressed in senior service college-level education and similar senior leader education programs. This workshop was designed to acknowledge and leverage existing education programs and to identify new programs and curricula that need to be developed. "Have to know" topics, as well as "nice to know" topics, were identified. These topics were further categorized by subject and the educational methodology that would best facilitate senior leader education.

The workshop established the foundation for discussion with plenary presentations from senior Cyberspace Operations practitioners as well as military, government and commercial subject matter experts. Invited cyber experts from the Department of Defense (DoD), the Department of Homeland Security (DHS), academia, and commercial organizations were divided into three workgroups: Cyber Threats and Vulnerabilities, National and International Critical Infrastructure Issues, and Preparation for a Catastrophic Event. Workgroup participants were tasked to discuss and compile topic areas that are considered critical to senior leader education and to consider the appropriate educational methodology. The initial results of the workshop were briefed to the Chief of Staff of the U.S. Strategic Command, Major General Abraham Turner, who provided his perspective on cyberspace operations and the preparation of senior leadership.

This report divided into in five sections: 1) workshop overview and objectives, 2) report of the plenary sessions, 3) workshop working group findings and reports, 4) workshop outbrief, and 5) final conclusions and recommendations.

SECTION 1: OVERVIEW AND OBJECTIVES

The demands of successful senior leadership in the United States now requires knowledge and decision making expertise in cyberspace operations. Government agencies, commercial enterprises, and academic institutions are heavily reliant on the Internet and other networks for information sharing. These networks are a battle space for information security and network capability as a variety of threats continuously disrupt the flow of information required for both commercial exchanges and military operations. These threats could be as sinister as combative nation-states, or could be as simple as malicious "script kiddies" or individual hackers. Cyberspace transcends the traditional nature of military domains (the other domains are Air, Land, Sea and Space) as it is a man-made domain. Actions taken in cyberspace can occur

in any and all other domains at the same time. Cyberspace operations are not constrained by the other domains. Further, cyberspace extends past normal military considerations as the structure of the networks is about 85 percent commercially owned and operated. Finally, existing international laws and charters do not directly address cyber war, causing great confusion and debate.

The significance of cyberspace to warfighting has reached a point where senior military leaders need to consider cyberspace issues in Commanders Critical Information Requirements (CCIRs) as they can significantly impact the effectiveness of military organizations. The responsibility of making cyber related decisions can no longer be passed to the communications officer because these decisions must be made within the context of the organization's operational mission. Intelligence, operations, logistics, and plans organizations are all greatly affected by the availability and security of cyber space systems. Response to attacks, network configuration and security, and relationships to other units are all affected by the commander's decision making concerning the utilization of his cyberspace capabilities. Additionally, since it is possible in a cyber attack to lose some network functionality, an organization's preparation for network operations in a degraded mode can be critical to success.

Educating future senior leaders is one of the many responsibilities of academia. In the military, the senior service colleges have the task of preparing future senior leaders. Due to the depth of knowledge required for senior leadership and the limited time available to students at the senior service colleges, competition for time in the curriculum is intense. Modern cyberspace operations include emerging threats, and, as a newcomer to the fight, the significance of these operations needs to be demonstrated in order to get them inserted into service college curriculum and Joint Professional Military Education (JPME) requirements. This workshop was designed to identify strategic issues in cyberspace operations that can be brought to the attention of those who define JPME requirements.

There are many aspects of cyberspace operations in military planning and execution, so the workshop focused on three overarching topics that could cover the "playing field" and from them develop specific issues that required academic attention. These three significant areas, as previously mentioned were: threat and vulnerability, infrastructure issues at the national and international levels, and the preparation for a catastrophic event. Plenary speakers provided a background and overview of each of the topics, which then led to individual

work groups that considered the identified topics in detail. While the topics were intentionally wide in scope, each of the work groups provided thoughtful consideration based on a series of related questions, and produced results that focused on the specific knowledge that future senior leadership will need as cyberspace continues to gather momentum as a potentially game-changing area of future warfare.

The work groups were provided with a series of overarching objectives focused on academic requirements in cyberspace operations. The threat and vulnerability group looked at security and information assurance issues, considered terms and definitions and strategy, and spent time identifying the "have to know" issues concerning cyberspace and national security. The infrastructure group considered the national and international laws and charters, current military and interagency infrastructure, and the topic of government to private industry relationships. They spent time reviewing current policies while developing those areas that senior leaders "have to know." Finally the catastrophic group considered what "catastrophic" really meant and the national security implications of such events, considering preparation, response, and recovery options for government organizations, especially military posts and units. This group also developed "have to know" issues for senior leadership.

SECTION 2: PLENARY SPEAKERS

In order to set the stage for the work groups the workshop featured subject matter experts in the areas of military cyberspace operations, government to civilian relationships, threat, Electromagnetic Pulse (EMP), and existing programs and objectives for senior leader education. The workshop started with a review of current military academia curricula on the subject, proceeded to briefings on the current status of the military with regard to the threat, and included several authors on the topics of cyber warfare and EMP.

Dr. Bert Frandsen, from the Air Force's Air University (AU), gave a presentation covering the multi-dimensional academic approach that the Air Force has implemented at AU. Some of these dimensions include training military lawyers in the legal aspects of cyberspace operations, conducting senior officer courses up to twice a year, and integrating cyberspace instruction into the command and staff college and AU curricula, both core and elective. Specific items of interest include a review of the writings of U.S. adversaries, discussions on the public-private relationships, and more specifically how the DoD fits

inside the Defense Support to Civilian Authority (DSCA) framework. The Air Force is ahead in the implementation strategy of cyberspace operations, but they are still looking for ways to expand their cyber academics to reach a wider audience.

Colonel Hal Arata, from the Air Force Institute of Technology, presented that school's program, which is a graduate-level education curriculum offering both masters and PhD level education. They have developed a new focus area with courses for cyber officers from Lieutenant to Lieutenant Colonel, with a goal of annually educating 600 (joint service) officers and civilians.

Dr. Chris Demchek, from the U.S. Naval War College (USNWC), discussed the capabilities and courseware of their cyber department. Currently the USNWC is conducting research and looking at the emergence of laws and policies, and the development of operational concepts in cyberspace that are related to those laws and policies. The school offers two courses in cyberspace operations, one on law and rules of engagement, and one on cyber security.

The Naval Postgraduate School's presentation was conducted via video teleconference. Their course structure is developed around providing graduate education in the areas of leadership, program management and operational effectiveness. They have six departments that provide academics toward a common cyber certificate. Perhaps of primary interest to this workshop was the Defense Analysis Department, which provides instruction in such areas as doctrine and strategy, threat assessment, cyberwar, and terror.

Finally, Mr. Bill Waddell, from the U.S. Army War College, discussed the first iterations of academics and exercises that were developed for academic year 2010 and the success of that initial courseware. Cyberspace instruction at the Army War College currently includes cyberspace material integrated into several core lessons and a classified elective course in cyberspace operations. These courses are maintained at the strategic level, providing students opportunity to understand the issues and vulnerabilities faced by the United States and its allies.

The workshop then turned to a series of plenary speakers, the first of which was Major General Steve Smith, Deputy Army G6 and the director of the Army Cyber Task Force. His organization provides forces for the Army Forces Cyber mission. Currently there is a lack of situational awareness across the elements of cyber operations, as there is no Title 10 mission to protect the civilian infrastructure. To be effective in cyberspace operations the operational

concepts need to be taken out of the "geek" channels and placed in operations and command channels. On the topic of educating senior leaders, MG Smith contended that the Army personnel offices need to relook assignment policy, as it takes about 3 years to train a 'hot' operator before the individual is moved to a new job, effectively losing the training investment. This loss of manpower investment will become critical over the next three years as the Army will become 80 percent continental United States (CONUS)-based. As a result of CONUS basing, mission planning needs to be done enroute, making expertise on network defense and attack more critical to ensure that this planning can be completed. What is first needed is a cyber common operational picture (COP), information assurance approved products (supply chain management), a robust certification and accreditation program, and collaboration between services on capabilities. Additionally, with regard to personnel, the training they receive needs to provide a cultural change (the current generation has less concern for security and more concern about through-put of information), providing focus on personal security accountability and awareness of threats, perhaps through an academic outreach program made available to all commands. The vulnerabilities of new social network capability (i.e. twitter, MySpace, Facebook, and many others) must become common knowledge, especially for military personnel.

Major General Smith stated that joint services need to begin testing systems and capabilities. He said there is a need for a cyber "competition" to get people interested in the research and development of new capabilities. He belives commanders must prepare their commands for conducting operations while under "cyber attack" or in degraded mode, and providing a list of issues for subordinate commanders to consider in the cyber arena. He concluded by demonstrating the vulnerability of private information by showing what information is available through Internet search engines; in this case what information could be gained about his boss by using Google searches.

The second plenary speaker was Brigadier General John Davis, the director of current operations (J33) of U.S. Cyber Command (USCYBERCOM). BG Davis outlined the responsibilities of USCYBERCOM and pointed out that the biggest challenge he faces is getting qualified personnel, because of the competition for them. USCYBERCOM is currently defining evolving relationships between all cyber players, as well as looking at clear definitions, laws and policies. In standing up USCYBERCOM, there are special relationships that need to be developed, such as with the Defense Information Systems

Agency that formerly directed Joint Task Force – Global Network Operations (the network defense portion of cyber operations). He also discussed the development of cyber support elements within the theater commands to provide liaison between the Theater planners and USCYBERCOM. The J33 is also developing similar liaison with the interagency and industry. BG Davis supports the development of a cyber COP and expressed concern about the current inadequacy of personnel and structure in defending the contested domain of cyberspace networks. He expressed the need for synchronization across the military and other agencies. Unity of vision, effort and commitment needs to be established, especially when dealing with limited resources. This synchronization is the only way to achieve the desired effects in support of military operations. The threat is not exaggerated; there is a great deal that needs to be accomplished to secure and protect the nation's cyber infrastructure.

The next speaker was Mr. Jeffery Carr, a cyber intelligence expert and author of the book "*Inside Cyber Warfare*" and principal, Greylogic. Mr. Carr discussed threats from both Russia and China, focusing on U.S. vulnerabilities. He discussed recent documents from both Russian and Chinese leadership concerning their proposed campaigns against U.S. targets. Of note was a recent research paper concerning U.S. electric blackouts and how to cause them. He also pointed out a series of unreported incidents through the year 2005 and discussed the origin of the incidents. Mr. Carr then discussed the vulnerabilities of existing energy system supervisory control and data acquisition systems, highlighting many of the vulnerabilities in this portion of critical infrastructure. His next topic was social networking vulnerabilities, where Mr. Carr illustrated how the targeting of individuals and organizations is conducted through the use of these new media. All of these areas need to become topics for a discussion between government and private industry and relationships need to be worked out to combat the many mutual threats.

The next speaker, Dr. Peter Pry, provided an assessment of the catastrophic vulnerabilities in our nation, specifically addressing the threat of electromagnetic pulse (EMP) weapons. He discussed the possibility of a massive cyber attack being the equivalent of a weapon of mass destruction (WMD) attack, and pointed out that cyber and EMP are part of the "bad guy" doctrine. Dr. Pry then discussed the mechanics of EMP, the vulnerability of our infrastructure to natural and man-made EMP, and the congressionally mandated commission on EMP that is assessing the threat. He noted that the national power grid is highly vulnerable to cyber or EMP attack, and the recovery time in the event

of a catastrophic event could take years. Dr. Pry encouraged the audience to prepare for a potential event. His recommendations included establishing a deterrent posture against attack, providing protection of critical components of key infrastructure, establishing a COP for critical infrastructures, recognizing EMP as a threat, and establishing a plan for systematic recovery in the case of attack.

Mr. Kevin Coleman, from Technolytics, spoke about government to industry relationships. Since the commercial sector owns and operates about 85% of the critical cyberspace infrastructure, Mr. Coleman contended that the government needs to establish a working relationship with industry, especially considering the number of commercial off the shelf products that DoD uses for their networks. Supply chain management to prevent the purchase and usage of counterfeit or malicious hardware has not been as robust as necessary. There are statistics that show a large and growing vulnerability in the area of counterfeit and malicious hardware. Additionally, Mr. Coleman stated that potential adversary nations are undertaking steps that will lead to an increasing vulnerability in this area, as is evident with China's recent laws requiring product vendors to submit details of the inner workings of 13 categories of security products before selling them in Chinese markets. He believes there needs to be working relationships across government and industry in order to determine the details of cyber defense/security policy, to include a mutual understanding of responsiblities for response to hostile actions against U.S. assets. This cannot be done without all parties working together, and the appropriate time to prepare is before, not during, hostilities.

Finally, to set the stage for the working groups, Colonel Jeff Caton, from the USAWC Department of Command, Leadership and Management, spoke on the topic of what senior military leaders need to know about cyberspace operations. He addressed the DoD definitions and characteristics of cyberspace and the levels of cyberspace operations. He discussed each of the three workshop areas and prepared workshop participants for their discussions and deliberations. He concluded by discussing overarching cyberspace issues, including the development of theory, who's in charge, normalization of the commons, and preparation.

Each of the speakers was very clear on several points: the threat is real and growing; cyberspace is a battlespace; the United States is vulnerable and that vulnerability is increasing; U.S. participants in the cyberspace security effort

must establish "unity of effort" and work together; and we must prepare now for cyber warfare. These are all senior leadership issues, as future success in both government and industry will require leaders and visionaries that understand the threat and vulnerability, can work inside the established national and international infrastructures, and who are prepared for potentially catastrophic scenarios.

SECTION 3: WORK GROUP SESSIONS

After the plenary sessions concluded participants split into their work groups to conduct further detailed discussion. The report of these work groups follows:

Threat and Vulnerability Work Group

1. Experience at the U.S. Army War College has demonstrated that senior leaders respond very positively to a description of the current threats in cyberspace which reveal a pattern of constant probing, infiltration, data compromise, and even physical damage. Recent experience in Estonia and during the 2008 Russia-Georgia War further validates the need to understand and engage on this vital topic. The outline which follows is meant to serve as a summary of key information senior leaders need to know concerning cyberspace threats and system vulnerabilities which impact national security and military operations.

2**.** *Cyberspace Operational Concepts and Definitions.* An understanding of the cyberspace domain in terms of a set of operational concepts and definitions is vital in order for senior leaders to visualize the relationship between the various elements. This visualization can often be a challenge to describe due to the inherent technical nature of the topic and the classification of some of the information related to it. Cyberspace has been defined as a man-made domain on-par with the other four physical domains (land, maritime, air, and space). The National Military Strategy for Cyberspace Operations defines the cyberspace domain as:

> *A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.*

a. Operational Environment. The operational environment consists of the five domains identified above along with the information environment.

The information environment as articulated in Joint Pub 3-13, *Information Operations*, cuts across all of the traditional domains and is described as consisting of:

(1) A physical dimension – the tangible real world where information systems (networks) operate

(2) An informational dimension – where information is created, manipulated, shared, and stored

(3) A cognitive dimension – which exists within the human mind where information is received, processed, and acted upon (decision-making) according to an individual set of perceptions, attitudes, and beliefs

(4) A social dimension – (not identified in JP 3-13) where human-beings interact and engage collectively consisting of:

(a) The User – the individual whose information and access to the network must be protected (considered either friendly or non-threatening)

(b) The Threat – those individuals attempting to gain access to protected or restricted information or to compromise the operation of information systems and networked infrastructure

b. Cyber Capabilities. Joint Pub 3-0, *Joint Operations*, defines cyberspace operations as being:

> *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.*

These capabilities can be thought of as being operationally focused (operate the global information grid), adversary focused (attack, defend, or exploit), or supportive of the previous two. This results in a framework consisting of:

(1) Cyber Net Ops.

(2) Cyber Attack/Exploitation/Dynamic Defense

(3) Cyber Support

c. *Cyber Effects.* Likewise, cyberspace operations effects can be focused on friendly information assurance or adversary capability reduction of escalating severity:

(1) Informational availability/protection/delivery

(2) Deny/Disrupt/Degrade/Destroy (the four D's)

3. *Threat Framework.* Specific examples or vignettes are helpful to both appreciate the nature of the threat and to understand the relationship between the types and methods of attack with the various system vulnerabilities that are being exploited. Ways of considering the threat are as follows:

a. Threat Payload and/or Effect: Denial of service (DOS), viruses, worms, trojans, botnets, etc.

b. Threat "Originators": The various threat actors (nation-state sponsored, non-nation-state, hackers, activitists, etc. How well can attribution be made? Can individuals be identified and "finger-printed" so as to be monitored over time?

c. Threat Strategies: What different strategies are being employed? Can they be further categorized?

d. "Means–Motive–Opportunity": Is this framework from law enforcement equally valid in the cyber realm? Is such anecdotal evidence sufficient for attribution and potential response action?

4. *Vulnerability Framework.* System vulnerabilities can be viewed as being primarily associated with either hardware, software, or the user.

a. Hardware (platform). Individual PCs, servers, DNS hosts, mobile devices, etc.

b. Software. Is validation of the operating system or the applications possible given the number of lines of code and the complexity of the system? What impact does out-sourcing programming (and manufacturing) have on the confidence that either have been compromised at the source?

c. User. What training do users require to properly safeguard both information and the integrity of the information system? How can threats from insiders be identified and mitigated?

5. *Impact on National Security Issues.* Some of the issues associated with cyberspace that impact national security are:

a. "DIME" Partnerships. The Diplomatic-Information-Military-Economic model for the elements of national power offers very little insight into the interdependencies among the power "elements" which is crucial to understanding the roles that cyberspace and cyberpower play.

b. Attribution Informs Deterrence. Effective deterrence in the cyber realm is critically linked to the ability to determine attribution for the intrusion or attack. Anonymous threats can neither be deterred nor punished appropriately after the fact.

c. Critical Infrastructure Protection. Nations which are critically dependent on the Internet for communications, commerce, power and water system distribution, etc., must protect those systems or risk the loss of vital infrastructure with a corresponding cascading set of adverse consequences. The loss of those systems will significantly impact the potential set of response options available to national leaders as well as divert assets away from punishing the aggressor to aiding the victims.

d. Increased Intelligence Requirements. Operating effectively in cyberspace demands accurate knowledge of both friendly and adversarial information system. Since these systems are highly dynamic and constantly changing, the demands on the intelligence community to keep up with them has never been greater. These requirements coupled with the classification levels necessary to protect this sensitive information are a tremendous challenge for both the intelligence and operational communities.

6. *Countermeasures.* Possible user countermeasures to mitigate the potential loss of information or the compromise of critical systems involve both a strategy and a set of actions to holistically respond to the possible threats.

a. Strategy. *Treat your most valuable data like you would treat your most valuable person*. Most users already know how to protect those they love and care about (children, family members, distinguished visitors, etc.). By extension the same considerations can be applied to protecting information and information systems in a way that both makes common sense and is easy to visualize.

b. Reduce your Attack Surface (Vulnerabilities). Applying the above strategy holistically involves considerations in three areas (similar to reducing the size of a triangle) – all of which must be addressed to reduce the overall vulnerability of information and information systems.

(1) Hardware. Both the devices themselves (through supply-chain management) and information system configuration must meet appropriate standards for safe and secure computing.

(2) Software. All software running on the system must be up-to-date and fully patched to reduce the potential for exploitation of known

vulnerabilities. Dangerous applications (peer-to-peer, etc.) must not be allowed on the system.

(3) User. All users need to take proactive steps to safeguard their systems from both human threats (hackers, robbers, etc.) and physical threats (acts of God).

(a) Identify Critical Data. Backup critical data regularly and store separately from the primary system. Use passwords and encryption to protect data at rest and in transit.

(b) Safe Computing Practices. Scan all disks before placing them in the system. Avoid questionable web-sites. Only open e-mail from known originators and scan all attachments.

(c) Real Time Monitoring. Be conscious of unusual system behavior (excessive hard-drive access, constant fan operating at high speed, sluggish response to input, etc.). Scan the system regularly for viruses, ad-ware, and mal-ware.

National and International Infrastructure Issues Work Group

In order to constrain the discussion, this group focused on two primary questions: (1) What do we expect our senior leaders to know about cyberspace operations, and (2) How should we educate them to ensure that they have this knowledge?

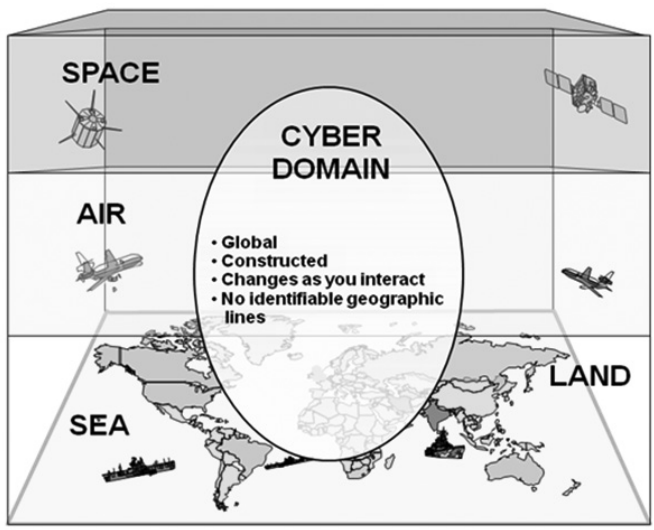

Figure 1: The Unique Nature of the Cyber Domain

The group began with a rapid review of senior leader education at the Senior Service College (SSC) level. Students trained in these institutions will be key staff officers and advisors to senior leaders in the short term, and will be key senior leaders for their organizations in the mid to long term. The group members acknowledged that the educational objective at a SSC cannot be to develop technically-skilled "cyber-warriors." Rather, it should be to educate "cyber-aware" senior leaders who have sufficient knowledge to understand basic cyber definitions and concepts and can then make logical and appropriate decisions on cyber issues when required to do so. The ability of other military educational institutions, such as the Air Force Institute of Technology or Naval Postgraduate School, to produce technically-skilled "cyber-warriors" was highlighted.

The group then noted the many inherent challenges in successfully educating SSC students on a domain that is so dynamic. Rapid changes in technologies, definitions and concepts, organization structures and missions, authorities and policies, and domestic and international laws all impact the knowledge base for cyber operations.

Question 1: What do we expect our senior leaders to know about cyberspace operations?

The group decided that there were basic definitions and concepts that needed to be taught as part of a core or basic senior leader education curriculum. Presentation of definitions of key cyber terms, especially "cyber warfare" and "cyberspace operations" is necessary, due to the ongoing debate on the meaning of these basic terms. In addition, the group agreed that there was a strong need for the development of a common cyber operations language – a cyber lexicon – so that all players (government, private, and international) can properly understand the dimensions of cyberspace and then collaborate successfully to address critical cyber issues. The group also agreed that basic cyber education should include an orientation on cyber defense, offense, organizations, policies, and capabilities, to include details of the various domestic and international authority and legal issues that impact what can be done, and by whom, in cyberspace.

The issue of how much knowledge of information technology (IT) should be taught created some contention within the group. While it is clear that younger generations are more comfortable with IT, it is not clear that they are sufficiently technologically-skilled to fully understand critical cyber issues. The

challenges experienced in the Army War College's first cyberspace operations elective are representative, where roughly one-third of the class was very conversant with cyber issues and computer networking technology, one-third was moderately informed on these topics, and the remaining one-third was almost completely uninformed on any cyber-related topics, to include basic computer networking principles. In the end, the group consensus was that there was a need for basic education on computer networking operations so that senior leaders can make informed decisions on cyber defense and offense actions and fully understand the operational impacts of those decisions. A variety of options for this introductory training were reviewed, ranging from self-paced on-line education to a formal preparatory classroom course. There was no consensus on the best way to perform this education, however. The group also highlighted the impact of IT centralization within the various services, which has had the effect of removing much IT decision-making from local commanders, as well as the need for senior leaders to develop a backup plan for degraded operations as a result of their own cyber defense actions or successful threat cyber offense actions.

Much of the subsequent discussion revolved around cyber defense and offense issues. Group members noted that countering cyber threats is inherently all about risk management, as a network will always have cyber vulnerabilities and will be faced with constant cyber threats. As a result, senior leaders must understand the normal noise level for their cyberspace environment but must also be aware of what constitutes an anomaly or spike in that noise. In addition, they must understand that the potential quantity of cyber attacks from nation-states is low but the potential impact is high; conversely, the quantity of cyber attacks from other sources (criminals, hackers) is high but the potential impact is generally low. Leaders must understand that the United States is particularly cyber-dependent, and thus is very vulnerable to attacks on our cyber infrastructure. Throughout all cyber activities, senior leaders must understand that the key cyber problem is the challenge of rapidly and accurately determining cyber attack attribution, a necessary step prior to initiating any cyber offense actions.

The group discussion then shifted to the fact that complex problems in cyberspace defy simple solutions, as the technologies are ever-changing, threats are dynamic, and there are many players with significant equities. Senior leaders need to appreciate the various current methods for cooperation, communication, and collaboration, both at interagency and between public,

private, and international organizations. When feasible, whole of government approaches and improved international cooperation need to be applied to cyber operations. In addition, SSC students need to understand that there are 18 national critical infrastructure sectors of which over 80% are operated or owned by the private sector; the cascading effects of civilian critical infrastructure failures will eventually impact military facilities and operations. This issue is especially critical for military networks, which have great reliance on commercial communications networks, both terrestrial and satellite.

Two additional issues that the group discussed were the impact of the current U.S. science and engineering education (human capital) deficit, which will negatively impact everyone – military, government, and business – and the continued decline in U.S. research dollars which will negatively impact our future cyber competitiveness. While these issues are outside the direct purview of the DoD, government organizations will have to live with the resulting challenges to hiring cyber-skilled employees and procuring future computer technology. This situation is further exacerbated by the low-density/high-demand nature of cyber expertise – the U.S. government must determine improved methods to recruit and retain these highly skilled personnel.

Question 2: How should we educate future senior leaders to ensure that they have this knowledge?

With respect to a basic or core SSC curriculum, the group recommended the increased use of scenarios with integrated cyber components within existing curricula and experiential educational events, such as the Army War College's Strategic Decision Making Exercise. They also suggested that core curriculum cyber instruction should focus on the differences between cyber operations and traditional operations and then illustrate the integration of cyberspace and traditional operations. Finally, they noted that classroom instruction should show integration of cyberspace with other domains, while highlighting cyberspace's unique role as the only man-made domain. All members of the group understand the difficulty of adding additional cyber education opportunities within the core curriculum due to the many other competing educational requirements at the SSC level. However, there was also a general consensus that cyber threats may now be so significant that cyberspace operations should warrant a more dedicated focus within the SSC core curriculum.

The group recommended that the SSCs sustain use of cyber-focused elective(s) to provide greater depth on cyberspace issues to interested students, especially since these electives can be structured as U.S.-student only courses and can then be offered as classified courses, allowing much greater discussion on cyber defense and offense issues. In these elective courses, they further recommended the use of real-world cyber case studies to illustrate the importance and impact of cyber events. If available, a review of recent industry and government cyberspace incident "hot wash" reports on intrusions and responses would add further fidelity to cyber issue discussions. The group also noted the importance of knowing what is going on in both the public and private sectors. Along with visits to government cyber facilities, participants suggested that visits to network security operation centers of major local corporations would be valuable and very feasible, as every corporation is dealing with network intrusions on a daily basis and have developed cyber visualization and response capabilities. In addition, they suggested the use of guided lab discussions and mal-ware demonstrations to illustrate critical cyberspace concepts and appropriate responses.

Throughout the SSC curriculum, the group recommended the encouragement of student research and writing on cyberspace issues and suggested that adding a student cyberspace writing award could further encourage this type of research and writing. Other recommended supplementary cyber education methods include scheduling noon time lectures and brown bag discussions with cyberspace subject matter experts, expanded partnerships with other war colleges, Naval Postgraduate School, Air Force Institute of Technology, DHS, USCYBERCOM, civilian academia and industry to address specific cyberspace topics, and the possible use of SSC Fellows programs to include experiential education opportunities within the cyber industry. A final suggestion was to develop continuing education modules to help SSC graduates maintain currency on the cyber domain as it continues to evolve.

Preparation for a Catastrophic Event Work Group

Key findings of group: Cyberspace-related catastrophic events are not only feasible, but also plausible, and some will argue, inevitable. Current military and government policy, doctrine, and senior leader education may not adequately address the catastrophic scope of potential events. Fortunately, much of the effort required to mitigate the catastrophic events exist or are in progress, but they need their scope of effort expanded or more fully defined.

Proper education, preventative measures, and preplanned mitigation processes lessen the chance of a widespread cyberspace event from becoming a national (or international) catastrophy.

Examination of group study questions:

Terms and definitions. The group looked at three specific cyberspace threats:

a. Natual electromagnetic events (such as magnetic field disruptions caused by solar storms)

b. Internet-faciliatated events (attacks and accidents) that disrupt electrical control devices (such as disruptions of supervisory control and data acquistion [SCADA] systems)

c. EMP events

1. What is "catastrophic"? The group developed a spectrum chart (below) to illustrate the factors and scope of emergency events that may require the response of organizations at the local, state, and federal levels. The vertical axis of the diagram represents the number of people affected and the horizontal axis represents the time to recover from a given event. Some examples are weather events (such as floods and hurricanes), geological events (such as earthquakes or tsunamis), and biological events (such as an influenza outbreak). The group judged an event to be catastophic when the number of people affected was greater than that normally covered by a given federal response area and the time to recover was well beyond that of a localized disaster. Also, catastrophic events involve almost complete disruption of communications and other infrastrucutre (such as the electrical power grid).

Three feasible catastrophic events are illustrated in the diagram: high-end cyberspace attacks (such as shutting down the SCADA systems controlling nationwide power generation and control), solar eletromagnetic storms (such as the Carrington event of 1859 and similar geomagnetic storms that may occur during the maximum output period of the 11-year solar cycle), and high-altitude nuclear EMP attacks that would have nationwide effects (such as that demonstrated in the U.S. Operation Fishbowl series of nuclear tests in 1962).

2. Preparations. The group identified several proactive measures to address potential catastrophic cyberspace events:

- Provide for an active and integrated cyber defense posture, integrated across the public and private sector. Properly implemented, this should help to reduce the spread of the effects, aid situational awareness, and encourage transparency of action.

- Consider expanding current emergency preparedness to the concept of "1950's" civil defense to include prepositioning of materials and stocks. These are prudent measures to help distribute the burden of supplying essential material (food, water, fuel, etc.) more evenly during any event and emphasis the benefits of individual citizen preparedness.

- Legislation to protect critical cyber related infrastructure (e.g., implementation of House Resoluton 5026, Electrical Grid Protection). Such actions are being considered by the current session of Congress.

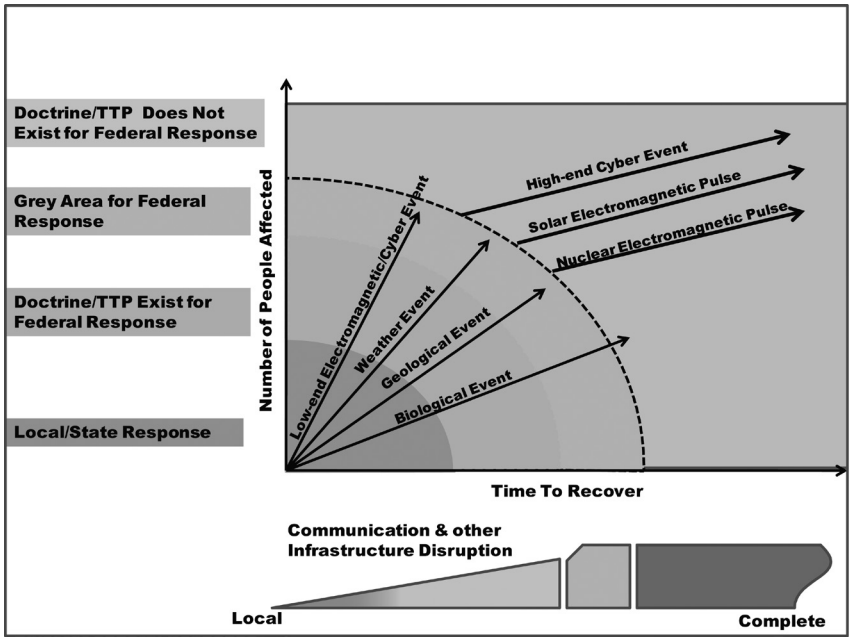

Figure 2: A Spectrum of Catastrophic Events

3. International implications. Although the group focused primarily on internal U.S. actions, it also touched on several issues with global effects:

- Develop a deterrence protocol for cyberspace and EMP threats. Consider a clear and unambiguous policy, primarily directed toward nation-states.

- Establish international protocols across all elements of national power. Consider existing treaties and law (such as the Law of Armed Conflict) as well as alliances (such as NATO).

- Consider retaliatory action based on established and exercised protocols. Any such actions should not be *ad hoc*, rather, they should be thought out and tested (using simulations or wargames) well in advance to assess potential second- and third-order effects.

4. Doctrine and planning needs. The group recognized the need to establish and evolve tenets and guidelines for operations related to catastrophic cyberspace events:

- Expand and exercise existing contingency and reconstitution plans to address catastrophic infrastructure loss (e.g., update National Response Framework). This may not require a complete rewrite, but rather an expansion of scope to encompass catastrophies. During the outbrief of the group findings, it was discovered that an interagency effort is underway to accomplish this and develop a National Cyber Incident Response Plan.

- Implement a pre-positioned and robust public information campaign. There was group consensus that an essential part of any cyberspace catastrophy response must include immediate and well coordinated communication nationwide to reduce any initial panic and uncertainty.

- Activate military bases as designated "Islands of Recovery." This concept is the cornerstone of the recovery strategy—as such, they must be identified and resourced well in advance.

- Implement roles and responsibilities of public and private sector to include jurisdictional authorities in accordance with National Response Framework. This should be planned with an all-of-government and all-of-private sector considerations.

5. What areas are "Have-to-know," what are the implication academically, and what is the best methodology to accomplish?

- Students must know that all national elements of power (diplomatic, information, military, and economic) must be considered in developing strategies and plans to address cyberspace catastrophies. They must also know the chacteristics of cyberspace and relationship to other domains

/strategic commons (i.e., air, space, and sea). They must appreciate the feasibility and plausibility of potential cyberspace events to have immediate and widespread catastrophic effects. And students must understand their potential roles in supporting proactive preventation measures as well as reactive mitigation actions.

- The best way to accomplish the education of these issues is by having them integrated throughout existing curricula. If appropriate, there can be a dedicated lesson on the basic characteristics and theory of cyberspace to provide a foundation for application. Cyberspace inputs into student exercises scenarios, ranging from small "table top" to more elaborate "multi-cell" exercises, can provide an opportunity for such application. For example, a catastrophic cyberspace event may provide an excellent scenario for applying material during DSCA lessons. Elective courses can provide a deeper knowledge base for students that require a more detailed understanding. Faculty-sponsored student research can help to expand the cyberspace knowledge base for the national security community writ large.

6. How should service college faculty be educated & prepared to present Cyberspace issues?

- Understand specific facts on the overall characteristics and effects of cyberspace events.
- Knowledge of current cyberspace-related efforts of U.S. and international organizations (such as USSTRATCOM and its USCYBERCOM, DHS, USNORTHCOM, etc).
- State of current doctrine with respect to not only areas such as cyberspace and information warfare, but also such areas as DSCA.
- Encourage development of cyberspace theory.

7. What additions/changes to JPME are needed to prepare senior leaders in SSCs and other academic institutions?

- Emphasize cyberspace in the context of traditional military theory, planning, and operations, that is, as an integral part of the profession of arms.
- Better integration among exisiting cyberspace centers of excellence (such as the Air Force Institute of Technology, Naval Postgraduate School, National

Defense University, etc). Consider the development of a standing working group on cyberspace.

- Emphasize the role of senior and strategic leaders as potential advisors with respect to cyberspace events (as opposed to tactical practitioners).

SECTION 4: WORKSHOP OUTBRIEF

On the final day of the workshop each work group leader provided a briefing to Major General Abraham Turner, Chief of Staff, U.S. Strategic Command. His remarks are summarized as follows:

The area of threat and vulnerability as well as the appropriate dynamic defense is still being debated, as are the definitions for cyber warfare. We are currently in the middle space between network operations and cyber war, but there is great concern that there is no declared policy on cyber war. One way to make the future better is through educating our leadership to be aware of the capabilities, conduct and culture of cyberspace operations. Currently the United States is digitally challenged, due to the issues of cyber lexicon and language. We must lay out and decide upon all the competing titles and authorities and state what we really mean so that there is no confusion between organizations. Student research will be very valuable to get all participants on the "same sheet of music."

Major General Turner stated that clearly the age of cyberspace is upon us, and he referenced the use of cyber war in the nations of Georgia and Estonia. He addressed the preparations at USSTRATCOM in the three areas of defense: high end cyber threat, solar and EMP. The development of dynamic defense, including the ability to function during an attack is critical. He pointed out that the development of a National Incident Response Plan is critical, and that it should also include the area of establishing a deterrence posture.

As we look to the future, Major General Turner provided three areas where academia should play a major role: bringing industry and bright minds into the fight, engaging international partners to get their input and coordination, and engaging academia to look at future concepts and requirements. Further, he stressed that we must dynamically defend the net and be able to thwart attacks quickly, we must prepare to work with local authorities in time of national emergency, and we must establish strong liaison with allied nations. We must all be diligent to prepare and have a clear understanding of what is at

stake. This should be a Congressional issue, one that makes it worthy of being on the "front burner."

SECTION 5: CONCLUSIONS AND RECOMMENDATIONS

Throughout this workshop the significance of cyberspace and EMP threats to the U.S. population was very apparent. This emerging battlespace is becoming hotly contested and presents many challenges that senior leaders must face. As noted in several of the sessions, DoD may be called upon to provide defensive, and possibly offensive, actions for the security of commercial networks, which means that the concept of warfare in the cyber domain will take on many new facets. Some of these include the required relationships with commercial and private entities, the challenges of interpreting existing national and international laws and charters, and technical challenges such as establishing a deterrent posture without clear attack attribution. As strategies and policies are being developed at the executive level, many organizations in the fight, especially geographic commands and homeland security organizations, find themselves having to develop their own doctrine in order to meet the emerging challenges. This lack of top cover and doctrine creates significant issues, as in some instances there is no legal basis for the conduct of operations while vulnerabilities may be left unprotected due to lack of policy.

Emerging senior leaders will face these issues directly in their military, interagency, and commercial organizations. It was the consensus of the groups that these future leaders are not being prepared for the cyberspace issues they will face now and in the future. Without clear strategy and policy, individual leaders' personal knowledge of cyberspace operations will be a major factor in their success or failure. Leaders have the obligation to prepare their organizations to meet the obstacles before them, but they must be aware of those obstacles in order to be successful. There is much confusion in definitions, authorities, lawful reactions to attacks, and other significant areas. This confusion is exacerbated when the senior leader is not appropriately educated on these issues.

The following recommendations were made by the workshop's work groups:

1. Cyberspace is a unique domain that traverses and affects all the other warfare domains. The application of cyberspace operational concepts within full spectrum operations and planning needs to be included in courses that develop senior leaders.

2. Realizing the limited time that students have at the senior service colleges and the extreme competition for contact time, recommend that the Joint Staff J7 establish education in cyberspace policy, strategy and operations as a priority in Joint Professional Military Education. Contact and academic time needs to be established for the teaching of cyberspace operations and concepts.

3. A full understanding of the threat of cyber attack, terrorism, or full warfare needs to be included in threat education for senior leadership. This education should also include concepts of the speed in which events happen in cyberspace. The threat of EMP should also be included in this education.

4. Senior leaders need to be aware of the application of cyberspace relative to existing laws and charters, i.e. the Laws of Armed Conflict, UN Charter, NATO Charter, etc. There are many nuances written in these laws that need to be understood by leaders making operational decisions, especially concerning the second and third order effects of decisions.

5. Preparation for the threat of attack and how to continue to operate in a degraded condition needs to be included in the education of senior leaders.

6. Educational programs needs to teach commanders how to include the entire scope of cyberspace operations in real "commander's business", and not delegate the responsibilities to subordinates.

7. As the U.S. Congress begins to pass laws and resolutions concerning the preparation for catastrophic events (e.g. HR 5026) leaders need to have an in-depth understanding of the requirements for recovery from these events.

8. Senior Service Colleges should establish liaison with commercial and academic organizations with similar objectives for senior leader education with the objective established to develop cross-culture education.

9. Those military academic organizations that are teaching cyberspace issues need to start a collaboration and sharing process, as clearly some institutions are ahead of others in the development of curricula for cyberspace operations and the preparation of senior leaders. Establishment of a formal cyber education consortium should be pursued.


Prudens
Futuri

The United States Army War College
Carlisle Pennsylvania

http://www.carlisle.army.mil