Strategy Research Project

COMMAND AND CONTROL OF THE DEPARTMENT OF DEFENSE IN CYBERSPACE

BY

CAPTAIN FRANK A. SHAUL
United States Navy

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
24-03-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Command and Control of the Department of Defense in Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Captain Frank A. Shaul

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Associate Professor Jeff Caton

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper examines current national cyberspace strategy and its implementation throughout the Department of Defense (DoD), the Service components and the Department of Homeland Security (DHS). Understanding the ordered effects of cyberspace will assist our nation's leaders, DoD, and DHS to develop and implement policy and structure for effective command and control of the nation's cyberspace resources to achieve national security objectives. To develop, implement, and sustain a viable strategy for cyberspace DoD leadership must focus defense policy on resources required to develop military and civilian leadership, and to train our military forces to defend the global information grid and assist in the protection of commercial networks as necessary to defend U.S. interests. Based on strategic guidance and the recent standup of United Sates Cyber Command (USCYBERCOM) and its mission to defend DoD networks, and to centralize command of cyberspace operations, Congress must authorize USCYBERCOM in coordination with DHS to act appropriately in defense of our nation's commercial and military information networks.

15. SUBJECT TERMS

Cyber Warfare, Strategy, Leadership, Defense, Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

COMMAND AND CONTROL OF THE DEPARTMENT OF DEFENSE IN CYBERSPACE

by

Captain Frank A. Shaul
United States Navy

Associate Professor Jeffrey L. Caton
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Captain Frank A. Shaul

TITLE: Command and Control of the Department of Defense in Cyberspace

FORMAT: Strategy Research Project

DATE: 24 March 2011 WORD COUNT: 5,881 PAGES: 30

KEY TERMS: Cyber Warfare, Strategy, Leadership, Defense, Security

CLASSIFICATION: Unclassified

This paper examines current national cyberspace strategy and its implementation throughout the Department of Defense (DoD), the Service components and the Department of Homeland Security (DHS). Understanding the ordered effects of cyberspace will assist our nation's leaders, DoD, and DHS to develop and implement policy and structure for effective command and control of the nation's cyberspace resources to achieve national security objectives. To develop, implement, and sustain a viable strategy for cyberspace DoD leadership must focus defense policy on resources required to develop military and civilian leadership, and to train our military forces to defend the global information grid and assist in the protection of commercial networks as necessary to defend U.S. interests. Based on strategic guidance and the recent standup of United States Cyber Command (USCYBERCOM) and its mission to defend DoD networks and to centralize command of cyberspace operations, Congress must authorize USCYBERCOM in coordination with DHS to act appropriately in defense of our nation's commercial and military information networks.

COMMAND AND CONTROL OF THE DEPARTMENT OF DEFENSE IN CYBERSPACE

This paper examines current national and Department of Defense (DoD) cyberspace strategy and its implementation throughout the DoD, the Service components and the Department of Homeland Security (DHS). It will also examine how the U.S. government has organized its cyber resources to command, control and defend DoD information networks effectively from a growing array of state and non-state actors in cyberspace. DoD currently defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] The Quadrennial Roles and Missions Review Report (QRM) of January 2009 states that, "Cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, inexpensively, and anonymously."[2]

The command and control (C2) of cyberspace is as much about secure infrastructure and networks as it is about the leadership and workforce that support and defend the freedom of access and critical flow of information in the cyber domain. Furthermore, the strategic command and control structure of cyberspace must develop resources to employ a joint military and civilian information dominance corps, made up of trained cyber warriors that are supported by dynamic lines of authority and tasked as an integrated cyber warfare ready response team. Based on strategic guidance and the recent standup of United States Cyber Command (USCYBERCOM) and its mission to

defend DoD networks, and to centralize command of cyberspace operations, Congress must authorize USCYBERCOM in coordination with DHS to act appropriately in defense of our nation's commercial and military information networks.

Cyberspace Strategy

According to James A. Lewis, on the Senate Committee on Commerce, Science, and Transportation, Cybersecurity, networked and digital information technologies provide the national infrastructure new ways to organize, interact and create wealth– actions that can now take place in cyberspace.[3] The 2010 Quadrennial Defense Review (QDR) describes cyberspace as a critical part of the global commons on par with land, air, sea and space realms of interchange.[4] Analogous to the U.S. Navy in keeping the sea lines of communication secure and open for free and unfettered shipping commerce; cyberspace has now become the common connector for transactional trade and commerce, thus it has become an essential path to global economic stability and national security. According to the National Security Strategy (NSS) of May 2010, cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The same technologies and networks that enable our military superiority are also unclassified and constantly probed by intruders and cyber criminals.[5] To secure and defend our nation from cyber attacks and conduct small or large scale military operations, the armed forces need to operate in cyberspace and defend cyberspace just as they would on land, in the air, or at sea. Neither government nor the private sector nor individual citizens can meet this challenge alone.[6]

To this end, the military requires resilient, reliable information systems and communications networks and unfettered access to the cyberspace domain.[7] The 2010 QDR states the DoD is taking several steps to strengthen capabilities in cyberspace to:

- Develop a more comprehensive approach to DoD operations in cyberspace;
- develop greater expertise and awareness;
- centralize command of cyber operations; and
- enhance partnerships with other agencies and governments.[8]

Developing and maintaining a joint cyber strategy will provide dynamic and flexible C2 needed to provide assured access to the global commons and cyberspace. According to the National Military Strategy (NMS) of 2011, Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force.[9] Articulating a Joint Force strategy in cyberspace is necessary, as cyberspace becomes a core competency of the armed forces. Most importantly, the leadership needed to continue to develop and carry out a Joint Force strategy will determine if we can achieve objectives in cyberspace, as defined by NSS 2010, QDR 2010, and NMS 2011. Our strategy and leadership in cyberspace must include an expanded means to provide information to our allies and to develop partnerships with a diverse population of actors found throughout the cyberspace domain. Moreover, operating effectively in cyberspace will need strategic leaders that can understand and apply resources of both people and technology to this vast and growing domain.

According to Presidential Cyberspace Policy Review, the threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies.[10] The case for organization and dynamic C2 of our nation's cyber resources stems from President Obama's directed review of cyberspace policy and the growing need to defend a highly technical domain critical to economic prosperity and military information superiority. To protect these critical economic sectors and governmental agencies from decay or loss, the NSS of 2010 states that as a nation we will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by: investing in people and technology and by strengthening partnerships.[11] As vague and broad as this statement is, our strategy must define the requirement from an organizational standpoint and install a C2 structure that can lead this effort with the resources and capabilities of trusted partnerships from DoD, DHS, National Security Agency (NSA), Defense Industrial Base, Science and Technology (S&T), and our allies and international partners.

General Keith Alexander, Commander of USCYBERCOM, in his recent testimony to congress stated, "In 2009, there were more than 1.8 billion internet users, and 4.6 billion cellular subscribers; together they sent roughly 90 trillion e-mails."[12] As stated in the National Military Strategy of 2011, the cyber threat is expanded and exacerbated by the lack of international norms, difficulties of attribution, low barriers to entry, and the relative ease of developing potent capabilities.[13] Cyberspace enables nation-states to conduct espionage and employ cyber warfare to attack other states or entities, either solely in the cyber domain or as part of a full-spectrum military maneuver.[14] Understanding the motive and ordered effects of cyber attacks will assist

our nation's leaders to develop national and international cyber law, cyber defense, cyber warfare rules of engagement, and when an attack warrants the need for an immediate non-kinetic response.[15] To answer cyber operational needs our computer network exploitation and defense capabilities must keep pace with the rapid advances in computer network technology and the cyber analytical tools needed to defend and counter threats and crimes in cyberspace.

Cyber warfare in the form of exploiting and attacking critical infrastructure has the potential to cripple a nation's power grid, its financial resources or even its military networks and its operating forces, all of which can become a threat to national security. Cyber warfare may be used as a means to exploit and infiltrate critical information systems to conduct industrial, technology and military espionage. The wicked problem that surrounds cyber warfare is twofold. First, because of the distributed nature of the Internet it is sometimes difficult to determine who originated the attack and the motive of the attacking party. Second, without a clear understanding of motive it is unclear when a specific act of unlawful or unethical cyber behavior would be considered an act of aggression. The rules of engagement as they relate to international law will require consensus and accountability from nations connected to cyberspace. One could argue that nations may come to an agreement on what constitutes a cyber attack, but may never come to agreement on how to enforce policy and law in the cyberspace domain. As envisioned, state and non-state actors can complicate deterrence and accountability by extending their reach through advanced technologies that were once solely the domain of states.[16] Additionally, they are using technology to coordinate and operate globally to spread extremist ideologies and attack the United States and our allies.[17]

In an attempt to address strategic cyberspace issues, President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) of March 2010, by Presidential Directive 54/Homeland Security Directive 23 (NSPD-54/HSPD-23) in January 2008. This initiative was further adopted by President Obama, who determined the CNCI should become part of the U.S. strategy to combat cyber security issues.[18] In doing so, President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter.[19] Furthermore, to advance national cybersecurity, the CNCI articulates twelve initiatives that the US government must fund in order to improve and strengthen strategic capabilities within federal agencies and key functions to include criminal investigation, intelligence collection, analysis, and information assurance supporting national cybersecurity objectives. Of the twelve initiatives put forward in the CNCI, initiatives 1 - 3, 5 and 12, are specifically linked to the organization of DoD and federal cyber agencies, and the resources needed to monitor and respond to cyber attacks.

In short, CNCI #1 details the need for a single federal network enterprise with Trusted Internet Connections, managed by Office of Management and Budget (OMB) and Department of Homeland Security (DHS).[20] CNCI #2 deploys an Intrusion Detection System (IDS) across the Federal enterprise, known as Einstein 2 to monitor attempts to gain access to federal networks. Einstein 2 is managed by DHS and run by the US-Computer Emergency Readiness Team (US-CERT).[21] CNCI #3 deploys Einstein 3 an intrusion prevention system across the federal enterprise using dynamic defense, and is perhaps the most intrusive means to protect both government and civilian networks

from intrusion and malicious content.[22] DHS, US-CERT and NSA are working together to ensure civilian privacy protections are in place prior to operational deployment of Einstein 3. CNCI #5 enhances situational awareness by connecting six cyber operations centers responsible for carrying out U.S. cyber activities.[23] CNCI #12 defines the role of federal cyber agencies in the cybersecurity of critical infrastructure domains that are privately owned and operated, yet critical for use by DoD, the military services, and other federal agencies.[24] These initiatives when funded and implemented will play a key role in supporting the recommendations of President Obama's Cyberspace Policy Review of May 2009.[25]

Secretary of Defense Robert Gates in the QRM of January 2009, states the department's vision is to develop cyberspace capability that provides global situation awareness of cyberspace, U.S. freedom of action in cyberspace, the ability to provide war fighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civil authorities.[26] One could argue the Secretary of Defense is advocating that DoD should develop the capability to command and control cyberspace, especially when it's in the nation's interests to do so, yet the command and control of cyberspace throughout the global commons in concert with war fighting effects quickly becomes problematic and constrained from a resource perspective.

Arguably this guidance provides perception that DoD C2 of cyberspace on a global level could be controlled by the Department in a given geographical location, or for that matter allowed access to a foreign nation's networks in times of crisis. For example, recent unrest by the Egyptian people claiming human right violations and demanding former President Mubarak to step down were somewhat driven by social

networks. To respond to the unrest the Egyptian government shut down its own internet service providers and cell phone services on January 27, 2011 in an attempt to undermine the movement by interrupting the use of social networking and news services.[27] This action taken by the Egyptian government effectively cut off U.S. freedom of action and situational awareness in cyberspace in Egypt. According to the National Military Strategy of 2011:

> Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, non-government entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills. Should a large scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable. We must seek executive and congressional action to provide new authorities to enable effective action in cyberspace.[28]

In order to achieve situational awareness in cyberspace and the ability to provide war fighting effects within and through cyberspace, Secretary Gates has determined that it is appropriate for each Service to develop capabilities to conduct cyberspace operations; and that improvements are needed in training and education to field a professional force, and in command and control for cyberspace operations.[29] One could argue that achieving war fighting effects in cyberspace cannot be achieved by a single Service component or even a sub-unified command such as USCYBERCOM; success in this area can only be accomplished by a Joint Force that includes cooperation with DHS and collaboration with our allies. NMS 2011 states, the collective and interlinked domains of air, space and cyberspace are essential to the Joint Force projection and sustainment of power and ability to deter and defeat aggression.[30] Moreover, in a domain that already connects DoD, the services, and other government agencies, the Department must

pursue joint doctrine that supports joint training, funding, S&T, and exercises C2 of the service components as one integrated cyber response team.

Secretary Gates in the QRM stated, "Cyberspace offers the U.S. military unprecedented opportunities to shape and control the battlespace to achieve national objectives."[31] Again, using the Egyptian government example of shutting down internet and cellular services to stop information flow in a time of crisis will only exacerbate controlled access to cyberspace in a given geographic location. To counter this potential problem secure and reliable C2 of cyberspace and unfettered access to DoD networks has become critical to the success or failure of a Combatant Commander (CCDR) operating in cyberspace. However, DoD dependence on C2 of external networks to prevent conflict or to support of full-spectrum military operations may remain problematic at best.

Command and Control of Cyberspace

Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint force.[32] Who is in charge of cyberspace when an attack or a disruption occurs in the continental U.S. or overseas in a U.S. territory, or on a DoD installation or network? According to Joint Publication 3-27, homeland defense falls under DoD action, whereas civil support is assigned to DHS or Department of Justice (DoJ)[33]. In the cyber domain this line of authority and responsibility can become blurred as cyber crimes and cyber attacks can originate from a myriad of sources from within the U.S. or outside of U.S. borders and its territories. Today there are a handful of U.S. government organizations working to defend and secure the nation's and DoD networks from cyber attack. In comparison,

there are a multitude of organizations, foreign governments, state and non-state actors, terrorists, and other criminal elements that provide a potential threat to national cyber security.

DHS is a cabinet level department created to address U.S. homeland security. Within DHS is the National Cyber Security Center (NCSC) and United States - Computer Emergency Response Team (U.S.-CERT). Specifically, DHS is responsible for securing the networks of the Federal Executive Branch civilian departments and agencies, often called the dot-gov domain.[34] DHS also works closely with partners across government and in industry to assist with the protection of private sector critical infrastructure networks.[35] They are tasked with protecting the U.S. government's communications networks, monitoring, collecting and sharing information on systems belonging to NSA, FBI, DoD, and DHS. The Department has a number of foundational and forward looking efforts under way, many of which stem from the CNCI.[36] US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS and responsible for providing response support and defense against cyber attacks for the Federal Civil Executive Branch and information sharing and collaboration with state and local government, industry and international partners.[37]

In support of USCYBERCOM mission to protect DoD networks and to achieve objectives outlined in the CNCI, the Secretary of Defense and Secretary of Homeland Security signed a memorandum of agreement that outlines terms by which DHS and DoD will provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of

current operational cybersecurity mission activities.[38] Key to implementation of this agreement will be the organizations ability within DoD and DHS to coordinate lines of operation that are mutually supporting and work to increase capacity and capability for both homeland and national security missions, while providing integral protection for privacy, civil rights, and civil liberties.[39]

In comparison, USCYBERCOM is a sub-unified command under US Strategic Command and tasked with centralizing command of cyberspace operations and strengthening DoD cyberspace capabilities. USCYBERCOM directs operations and defends the global information grid (GIG) in support of the DoD missions, executes full-spectrum cyber operations on command, and defends our nation's freedom of action in cyberspace.[40] USCYBERCOM is also responsible for planning, executing, and coordinating computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE) operations. However, effective C2 of cyber resources and the service component commands will be the critical linkage to enable securing cyberspace for DoD and the nation. In a statement before the House Committee Armed Services, General Keith Alexander articulates the wisdom of keeping command and control of military networks and operations with an organization possessing a global perspective on vulnerabilities, threats, and challenges to our nation; that is why U.S. Strategic Command, within the DoD, delegated cyberspace operations to USCYBERCOM.[41]

The standup of USCYBERCOM and the service components must go beyond a facelift reorganization of personnel and resources. To be effective, USCYBERCOM must develop and implement a strategy that pushes far past the boundaries of

information sharing and collaboration, and institute a truly comprehensive approach that compels its components to organize in a way that eliminates barriers and promotes innovation and cooperation. Not only must it synchronize operations within USCYBERCOM, but it must also synchronize operations with DoD, DHS, and other governmental agencies. USCYBERCOM must establish clear and unambiguous priorities that are codified in doctrine and hold the services accountable for developing capabilities that actually provide superiority and freedom of action in cyberspace. In other words DoD can no longer organize and then reorganize for the sake of standing up a new organization with a new name. The Goldwater-Nichols act of 1986 sought to meld the DoD tectonic divide between operational and administrative control of military forces.[42] The same kind of studied treatment must be given to cyberspace and the way it is fielded, maintained, commanded and controlled.[43] How USCYBERCOM organizes and implements C2 of its resources and DoD networks will make a significant impact on how DoD and the services operate in cyberspace.

US Fleet Cyber Command/Commander TENTH Fleet (C10F) is the US Navy component command to USCYBERCOM. To provide command and control and to enhance training and education to field a professional force, the Department of Navy (DoN) stood up Fleet Cyber Command[44] at Fort Meade, NSA. With the standup of Fleet Cyber Command/US TENTH Fleet it is apparent the DoN has shifted focus and budget toward building cyber capabilities through people and technology in order to carry out the DoD cyberspace objectives. FLTCYBERCOM is now responsible for cyber operations at 24 shore commands and for more than 45,000 active duty, reserve, and civilian personnel.[45] FLTCYBERCOM parallels other service cyber components, but also

has unique operational authority for networks, cryptology, signals intelligence, information operations, cyber, electronic warfare and space.[46] Because FLTCYBER is a service cryptologic component to NSA, and are headquartered at NSA, they are uniquely situated to carry out USCYBERCOM objectives and to collaborate face to face with the USCYBERCOM staff when necessary.

Additionally, Operational Navy (OPNAV) has reorganized its staff with the combining of the Intelligence (N2) and Networks (N6) directorates on October 1, 2009 and provided those organizations the programs and budgets to run them. Information Dominance Corps (IDC) was created to lead and manage a cadre of officers, enlisted, and civilian professionals who possess extensive skills in information-intensive fields.[47] This corps of professionals will receive extensive training, education, and work experience in information, intelligence, counterintelligence, human derived information, networks, space, and oceanographic disciplines.[48] The IDC will develop and deliver dominant information capabilities in support of U.S. Navy, Joint and National warfighting requirements. [49] Together the Deputy CNO for Information Dominance (OPNAV N2/N6) and Commander FLTCYBERCOM/C10F have elevated the role of information, cyber, space, and networks in the Navy's operations and investments, as a war fighting domain.[50] The reorganization and combining of staffs and Navy designators to establish the IDC provides a leadership framework and C2 structure to focus unity of effort for defending cyberspace and supports the NMS. The formation of the IDC is probably the most powerful part of the combined package to achieve cyberspace war fighting effects for USCYBERCOM and the Navy; however, it is also the most vulnerable due to the potential for cultural clashes and stovepipes to drive solutions. To overcome these

barriers to innovation, IDC leadership must provide a vision that empowers its people to innovate. Meanwhile the IDC must develop a professional force structure that is trained and ready to fight and win the nation's wars in cyberspace.

Army Forces Cyber Command (ARFORCYBER) is the US Army component command to USCYBERCOM. Headquartered at Fort Belvoir, Virginia, ARFORCYBER's primary mission is to support USCYBERCOM in its defense of DoD networks and the nation's networks. Led by Major General Rhett Hernandez, ARFORCYBER will command nearly 21,000 active military and civilian personnel around the globe.[51] His statement to congress clearly articulates the capability to operate in joint and international environments that include support to USCYBERCOM, the other service components and also other departments, agencies and private entities. Key to ARFORCYBER accomplishing the mission will be the linkages between sister services and balancing centralized C2 against Army and Joint theater missions. Key priorities are leveraging S&T and academia, rapid acquisition and testing of new capabilities, and rapid fielding of those technologies similar to rapid fielding efforts in Iraq and Afghanistan.

Twenty Fourth Air Force, headquartered at Lackland Air Force Base, Texas, is the US Air Force component command to USCYBERCOM. Major General Webber commands nearly 15,000 personnel and is tasked with defense of Air Force networks and cyber support to Combatant Commands.[52] Major General Webber argues in testimony, that the integration of cyber capabilities in support of Joint operations is absolutely essential.[53] His view of combating cyberspace is that of a team sport and must include close coordination and collaboration with sister services and

USCYBERCOM. As the other services are already doing, AFCYBER is also shifting its traditional reactive network to one that is more predicative and dynamic.

US Marine Corps Cyberspace Command (MARFORCYBER) is the US Marine Corps component command to USCYBERCOM. MARFORCYBER commands a staff of 800 personnel tasked with defense of the Marine Corps Enterprise Network.[54] MARFORCYBER intends to use its limited resources take care of its own force first. However, they are advocating to USCYBERCOM and the other Service components the need for a joint approach to equipping the force. While it is clear that the service components have stood up their individual organizations, it is not clear if joint training, resourced by service specific funding, acquisition, S&T, and doctrine will be able to support a decentralized C2 structure with centralized tasks and common objectives, yet grossly needed to defend DoD networks and the nation's networks from attack.

Leadership in Cyberspace

Cyber-strategic leadership is not a specific technical skill or person, but a set of knowledge, skills, and attributes essential to all leaders at all levels of government and in the private sector.[55] In an article published by The Heritage Foundation that discusses cyber leadership in the twenty first century, Dr. James Carafano and Eric Sayers articulate:

> Even as Washington wrestles with issues concerning organizations, authorities, responsibilities, and programs to deal with cyber competition, it must place more emphasis on developing leaders who are competent to engage in these issues. This will require a professional development system that can provide a program of education, assignment, and accreditation to develop a corps of experienced, dedicated service professionals who have expertise in the breath of issues related to the cyber environment. This program must be backed by effective public-private partnerships that produce cutting-edge research, development,

> and capabilities to operate with freedom, safety, and security in the cyber world.[56]

In recent testimony by VADM Barry McCullough III, Commander U.S. Fleet Cyber Command/Commander U.S. Navy TENTH Fleet to the Terrorism and Unconventional Threats and Capabilities Subcommittee of the House Armed Services Committee, "the Navy's vision is to fully develop our ability to operate in cyberspace by fusing old - and developing new–capabilities and capacities across our networks, signal intelligence systems, and electronic warfare systems."[57] Within the Navy's intelligence communities there has always existed a disparate view on how to unify operations in the information warfare domain, especially between intelligence and information disciplines and how to best support the warfighter. With the recent standup of the IDC under the leadership of VADM Jack Dorsett (Intelligence Officer and Deputy Chief of Naval Operations for Information Dominance N2/N6), and U.S. Fleet Cyber Command/TENTH Fleet, VADM McCullough (Surface Warfare Officer), the vision or whole war fighting approach to how the Navy operates its combat capabilities in the cyberspace domain, takes on a strategic sense of urgency to get it right, now.[58]

Never before has the Chief of Naval Operations named a three-star Intelligence Officer and a three-star Surface Warfare Officer to lead and develop the Navy's Information Dominance Corps, and its cyber forces to accomplish the cyberspace mission. Admiral Mullen argues that, to shape the future force, we must grow leaders who can truly out-think and out-innovate adversaries while gaining trust, understanding, and cooperation from our partners in an ever-more complex and dynamic environment.[59] His argument is exactly what professional military leaders must do to get ahead and stay ahead of our competitors. In order for a strategic leader to effect change

in largely complex organizations he must have the capacity, at the strategic level, to envision the future. VADM Dorsett is a cyber strategic leader because he has provided that vision for the IDC and has offered to transform the Navy's information capabilities to deliver game-changing decision superiority and command and control overmatch.[60] Kotter argues that, "vision plays a key role in producing change by helping to direct, align, and inspire actions on the part of large numbers of people."[61] Vision provides a sense of ultimate purpose, direction, and motivation for all members and activities within an enterprise.[62] While providing vision may help to direct or align mission, it is not a substitute for getting the job done.

With the standup of Fleet Cyber Command, VADM McCullough has the complex task of adapting the Navy's cyber warfare vision to over 45,000 personnel. Through his strategic leadership he must adapt and better align Fleet Cyber Command with its rapidly changing and highly technological environment. His goal is to transform a highly technical, yet mostly static and reactive network operations capability, to a more proactive and dynamic capability. Burke infers that leadership is a personal matter, understanding more about the proper match between a leader's personality and the desired organizational culture is critical to successful change.[63] Achieving transformation and a unified vision will require a continued investment by senior navy leadership to develop the cyber force and to create a climate that will motivate the IDC and its culture to move with the changing tide of technology. At the strategic level, technical competencies include an understanding of organizational systems, an appreciation of functional relationships outside the organization, and knowledge of the broader political and social systems within which the organization operates.[64] VADM

McCullough's initial focus is on networks and how to command and control his cyber forces globally. His near term goal is to establish dynamic cyber operations, which includes defense, as well as exploitation and development of non-kinetic effects.

Now that VADM McCullough has shared the Navy's vision on cyber warfare with the House Armed Services Committee, and VADM Dorsett has shared his vision on information dominance with the Navy, they must develop definable objectives, concepts and resources to achieve the mission. Furthermore, one could argue that for real transformation to take place regarding the C2 of cyberspace, the four service components and USCYBERCOM will need to share and develop objectives and resources to achieve the mission. Thus, visions serve another purpose–that of accountability."[65] Accordingly, the espoused vision holds the strategic leader accountable to its employees and external stakeholders, as well as holding the organization accountable for maintaining structure, process, and alignment to the vision.[66]

Cyberspace Strategy

The major goal of the Comprehensive National Cybersecurity Initiative (CNCI) of March 2010 is to establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government, and ultimately with state, local, and tribal governments and private sector partners, and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.[67] In support of the CNCI, and according to the Quadrennial Defense Review of 2010, DoD is continuing to invest and improve capabilities in cyberspace by developing a more comprehensive approach to DoD operations in cyberspace in order to more effectively monitor and secure DoD networks

and commercial internet domains from cyber attacks. According to Admiral Mullen, Joint Forces will secure the ".mil" domain, requiring a resilient DoD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense.[68] The defense of cyberspace for the DoD and the nation, via oversight and coordination from DHS, are executed by the service components, therefore funding and modernization of USCYBERCOM and the service component cyber commands are critical to the securing of cyberspace for DoD and potentially for the nation.

Today USCYBERCOM is the Joint Force that has C2 authority and responsibility to defend DoD networks. This strategy allows DHS and other federal agencies (FBI, CIA, and NSA) to retain autonomy of their own cyber responsibilities, programs and budgets. One could argue this strategy is not acceptable as it promotes a pre-9/11 collection and sharing of intelligence information that is not transparent to other intelligence organizations, and does not appropriately secure the nation's private and public cyber domain. Maintaining stovepipe information systems and network sensors are costly and not conducive to a coordinated response or preemption of attack by DoD, federal agencies, and private organizations. Additionally, without full transparency of intelligence sharing and collaboration with USCYBERCOM and its military service components of nearly 82,000 combined personnel, the appropriate defense to the nation's cyber threats could go untreated. This strategy incurs high risk in areas of transparency, funding and prudent use of limited resources and does not meet the suitability objectives of CNCI #1, #5 and #12.

A second strategy considers USCYBERCOM as sole C2 authority and responsibility to defend DoD and U.S. public cyberspace domain. The acceptability and

feasibility of USCYBERCOM as the sole government cyber entity tasked with defending both DoD and public networks will be a hard sell for most private citizens and institutions due to privacy issues and a perceived lack of oversight. Buy-in from federal agencies such as DHS and FBI to relinquish their cyber responsibilities and resources would require considerable support from congress, the President, and would require a strong policy statement by the current administration. This option does not support suitability objectives of CNCI #1, #2, #3, #5 and #12, and assumes too much risk with one DoD organization responsible for monitoring cyber intrusions and defense of the networks for DoD and the nation.

To fight and win in cyberspace a third strategy that resources decisions as a single network must be carefully considered. A more robust and dynamic option must be put forward that elevates USCYBERCOM C2 of cyberspace in close partnership with DHS and coordination with other US federal agency partners (FBI, CIA, DoJ, NSA), and U.S. allies. This option gives USCYBERCOM the authority to defend DoD and the U.S. commercial cyber domain as necessary to protect national interests. This option will be acceptable to most private, public and federal agencies once buy-in by congress and federal agencies occur. Strategic communication will garner acceptability and buy-in from public and private institutions with emphasis on maintaining privacy for US citizens. This option meets suitability objectives for CNCI #1, #2, #3, #5 and #12, supports NSS, DoD, NMS, and QDR cyber space objectives to defend DoD networks and the GIG, and enables USCYBERCOM to use both offensive and defensive cyber weapons in defense of DoD, and the nation's public and private networks. Feasibility will be driven by Congress to commit significant resources of funding for new information systems and

training for network administrators and cyber analysts. This option reduces risk by decentralizing monitoring and cyber response activities, and promotes the need for a single federal network enterprise with Trusted Internet Connections that are truly compliant with industry standards. Additionally, this option provides a ready force of over 82,000 military intelligence and cyber experts.

Conclusion

A prosperous and interconnected world requires a stable and secure environment, the absence of territorial aggression or conflict between states, and reliable access to resources and cyberspace for stable markets.[69] Developing a strategic, yet flexible and dynamic organizational structure for DoD and DHS to respond to cyber attacks that pose a threat to national security, and to deter cyber acts of war through computer network defense in the cyber domain will be a challenge for many. Training and education in the cyber domain will assist both our cyber leaders and the cyber workforce to develop, implement, and sustain an organizational structure that addresses command and control issues and lead to development of national and international cyber law. It will also assist in developing military and civilian cyber leadership, develop a cyber deterrence policy, develop cyber attack rules of engagement, and develop our military forces to defend the global information grid, provide unclassified assistance to commercial network providers, and to exploit and attack cyber transgressions as necessary to defend U.S. interests.

Based on strategic guidance and the recent standup of USCYBERCOM and its mission to defend DoD networks and the GIG, and to centralize command of cyberspace operations, the third option would be the most prudent use of cyber

resources available today to protect and secure the nation's networks and ensure freedom of action in the cyber domain. To this end Congress must authorize DHS and USCYBERCOM to act appropriately in defense of our nation's commercial and military information networks. Additionally, Congress must authorize USCYBERCOM to use both offensive and defensive cyber weapons and the tools necessary to hunt down cyber criminals based on rule of law and the legal framework. The U.S. government must also establish cyber partnerships with international stakeholders, its allies, and all federal agencies. USCYBERCOM and its service components while conducting operations in cyberspace, must comply with oversight and compliance policy managed by DHS/NCSC. The third option best supports the President's National Security Strategy for 2010, the 2010 CNCI, DoD, QDR, and NMS objectives and enables our nation to prosper and grow in cyberspace, the fifth domain.

Endnotes

[1] U.S. Deputy Secretary of Defense Gordon England, "The Definition of 'Cyberspace," memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008.

[2] U.S. Secretary of Defense Robert M. Gates, "Quadrennial Roles and Missions Review Report," Department of Defense January 2009.

[3] U.S. Senate Committee on Commerce, Science , and Transportation, Cybersecurity – "Assessing Our Vulnerabilities and Developing an Effective Defense," *Center for Strategic and International Studies*, March 19, 2009.

[4] U.S. Secretary of Defense, Robert M. Gates, *Quadrennial Defense Review Report, (*Department of Defense February 2010), 37.

[5] Barrack H. Obama, *National Security Strategy*, (Washington DC: The White House, May 2010), 27.

[6] Ibid, 28.

[7] Barrack H. Obama, *Cyberspace Policy Review: Assuring a Trusted and Resilient Informations and Communications Infrastructure*, (Washington DC: The White House, May 2009), 1.

[8] Gates, Quadrennial Defense Review 2010, x.

[9] Mike G. Mullen, The National Military Strategy of the United States of America, Redefining America's Military Leadership, 2011.

[10] Obama, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

[11] Obama, National Security Strategy, 27-28.

[12] Statement of General Keith B. Alexander, Commander United States Cyber Command, before the House Committee on Armed Services (September 23, 2010).

[13] Mullen, National Military Strategy, 4.

[14] Ibid.

[15] A Non-kinetic response refers to cyber warfare or non-kinetic warfare as a form of low-intensity conflict during peacetime and offers the potential for impact without loss of life, http://www.infosectoday.com/Articles/Cyber-Warfare.htm (Accessed 19 March 2011).

[16] Mullen, National Military Strategy, 4.

[17] Ibid.

[18] Barrack H. Obama, "The Comprehensive National Cybersecurity Initiative," March 2, 2010, linked from *The Whitehouse Homepage* at "National Security council – Cybersecurity," http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed December 2, 2010).

[19] Ibid.

[20] Ibid., 2.

[21] Ibid., 2.

[22] Ibid., 3.

[23] Ibid., 3-4.

[24] Ibid., 5.

[25] Obama, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

[26] Gates, Quadrennial Roles and Missions Review Report, 14.

[27] Christopher Rhoads and Geoffrey Fowler, “Egypt Shuts Down Internet, Cell Phone Services,” *The Wall Street Journal*, http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html (accessed on February 2, 2011)

[28] Mullen, National Military Strategy, 10.

[29] Gates, Quadrennial Roles and Missions Review Report, 14.

[30] Mullen, National Military Strategy, 9.

[31] Gates, Quadrennial Roles and Missions Review Report, 15.

[32] Mullen, National Military Strategy, 9.

[33] Joint Chiefs of Staff Joint Publication 3-27, *Homeland Defense*, (July 12, 2007).

[34] Department of Homeland Security Cybersecurity Web page, http://www.dhs.gov/files/cybersecurity.shtm (accessed on 2 March 2011)

[35] Statement of Deputy Under Secretary Philip Reitinger and Deputy Assistant Secretary RADM Michael Brown, National Protection and Programs Directorate, before the House Appropriations Committee, on the Department of Homeland Security Fiscal Year 2011 Cybersecurity Budget, April 15, 2010.

[36] Ibid.

[37] Department of Homeland Security home page http://www.us-cert.gov/aboutus.html (accessed November 15, 2010).

[38] U.S. Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano, “Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,” October 13, 2010.

[39] Ibid.

[40] Statement of General Keith B. Alexander, Commander United States Cyber Command Before the House Committee on Armed Services, September 23, 2010.

[41] Ibid.

[42] Wesley R. Andrues, “What Cyber Command Must Do,” *Joint Force Quarterly*, 59, 4th Qtr 2010, 115.

[43] Ibid.

[44] Highlights of the Department of the Navy FY 2011 Budget, “Rebalancing to Meet Priorities,” Department of the Navy, 2010, 2.

[45] Gary Roughhead, “CNO Guidance for 2011, Executing the Maritime Strategy,” October 2010, 6.

[46] Statement of Commander, U.S. Fleet Cyber Command/Commander, U.S. TENTH Fleet to the Terrorism and Unconventional Threats and Capabilities subcommittee of the House Armed Services Committee, *Digital Domain: Organize the Military Departments for Cyber Operations,*September 23, 2010.

[47] Chief of Naval Operations, OPNAVINST 5300.12, *The Information Dominance Corps*, October 6, 2009.

[48] Ibid.

[49] Ibid., 1.

[50] Gary Roughhead, CNO Guidance, 6.

[51] Statement of Major General Rhett Hernandez, USA Incoming Commanding General, U.S. Army Forces Cyber Command Before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, 2nd Session, 111th Congress, September 23, 2010.

[52] Statement of Major General Richard E. Webber, USAF Commander Twenty Fourth Air Force (AFCYBER) Presentation to the Before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations,* September 23, 2010.

[53] Ibid, 9.

[54] Statement of Lieutenant General George J. Flynn Deputy Commandant for Combat Development and Integration Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee Concerning *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations,* September 23, 2010.

[55] James Jay Carafano, Ph.D., and Eric Sayers, "Building Cyber Security Leadership for the 21st Century," *Backgrounder*, The Heritage Foundation, December 16, 2008, 3.

[56] Ibid.

[57] Commander, U.S. Fleet Cyber Command/Commander, U.S. TENTH Fleet, to the Terrorism and Unconventional Threats and Capabilities subcommittee of the House Armed Services Committee, *Digital Domain: Organize the Military Departments for Cyber Operations,*September 23, 2010.

[58] VADM Bernard J. McCullough III, "Talking with Vice Admiral Bernard J. Barry McCullough III commander, U.S. Fleet Cyber Command/commander, U.S. 10th Fleet," *CHIPS* magazine*,* April 1, 2010, 4.

[59] Mullen, National Military Strategy, 16.

[60] David J. Dorsett, Deputy Chief of Naval Operations for Information Dominance N2/N6, *The U.S. Navy's Vision For Information Dominance*, May 2010, 1.

[61] John P. Kotter, *Leading Change* (Boston MA: Harvard Business School Press, 1996), 7.

[62] Stephen J. Gerras, *Strategic Leadership Primer*, (Carlisle PA:USAWC, 2004): 21.

[63] W. Warner Burke, "*Organizational Change: Theory and Practice,"* (Thousand Oaks , CA: Sage Publications Inc., 2011), 43.

[64] Gerras, *Strategic Leadership Primer*, 31.

[65] Kotter, *Leading Change*, 14.

[66] Ibid.

[67] Obama,The Comprehensive National Cybersecurity Initiative,1-2.

[68] Mullen, National Military Strategy, 19.

[69] Ibid., 7.