Strategy Research Project

What is the Mortar in the Department of Defense's Cyberforce Firewall?

by

Colonel Kenneth L. Cypher
United States Army

U.S. ARMY WAR COLLEGE
Prudens Futuri
Carlisle Barracks, PA

United States Army War College
Class of 2014

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

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.

REPORT DOCUMENTATION PAGE	*Form Approved--OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 15-04-2014	**2. REPORT TYPE** STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE What is the Mortar in the Department of Defense’s Cyberforce Firewall?	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Colonel Kenneth L. Cypher United States Army	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Professor William Waddell Director, Mission Command and Cyberspace Group	**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: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

Word Count: 5,129

14. ABSTRACT

The March 2013 Director of National Intelligence Worldwide Threat Assessment ranked cyber threats as the number one threat to National Security. The Department of Defense is working towards addressing the national security threat from cyberspace nefarious actors but, DoD is lethargic due to entrenched thoughts and bureaucratic processes. This paper addresses entrenched thoughts of network centricity. Network operations are not cyberspace combat operations. There are two distinct separate operational communities in cyberspace. Department of Defense information network operations are combat support, sustainment, and cyberspace resiliency operations. Defensive and offensive cyberspace operations are combat operations. Each community must have a distinctly different focus but must be under on command authority to ensure integration to defend the seams from adversary exploitation.

15. SUBJECT TERMS

Cyber Defense, Network Defense, Cyber Defense Operations, Cyberspace

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	32	**19b. TELEPHONE NUMBER** *(w/ area code)*

USAWC STRATEGY RESEARCH PROJECT

What is the Mortar in the Department of Defense's Cyberforce Firewall?

by

Colonel Kenneth L. Cypher
United States Army

Professor William Waddell
Director, Mission Command and Cyberspace Group
Project Adviser

This manuscript 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.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the United States Government.

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

Abstract

Title:	What is the Mortar in the Department of Defense's Cyberforce Firewall?
Report Date:	15 April 2014
Page Count:	32
Word Count:	5,129
Key Terms:	Cyber Defense, Network Defense, Cyber Defense Operations, Cyberspace
Classification:	Unclassified

The March 2013 Director of National Intelligence Worldwide Threat Assessment ranked cyber threats as the number one threat to National Security. The Department of Defense is working towards addressing the national security threat from cyberspace nefarious actors but, DoD is lethargic due to entrenched thoughts and bureaucratic processes. This paper addresses entrenched thoughts of network centricity. Network operations are not cyberspace combat operations. There are two distinct separate operational communities in cyberspace. Department of Defense information network operations are combat support, sustainment, and cyberspace resiliency operations. Defensive and offensive cyberspace operations are combat operations. Each community must have a distinctly different focus but must be under on command authority to ensure integration to defend the seams from adversary exploitation.

What is the Mortar in the Department of Defense's Cyberforce Firewall?

> We meet today at a transformational moment -- a moment in history when our interconnected world presents us, at once, with great promise but also great peril.
>
> —President Barack Obama[1]

The Cyberspace environment is a man made environment which presents greater opportunities to control and influence the environment. It also opens up greater access for nefarious activity and human error. Therefore, cyberspace requires care and feeding in order to conduct operations in and through that the other military operational domains of air, land, sea, and space do not require. Cyberspace continues to mature as an operational domain and environment much like air and space did in the time and space of decades vice centuries. This paper will propose thoughts to alleviate several points of confusion over cyberspace Department of Defense Information Network (DoDIN) operations and defense cyberspace operations (DCO). First, the cyberspace environment will be framed in order to provide a relevant understanding of the linkages between Joint Publication 3-12 and Army Field Manual 3-38 of the information environment, layers of cyberspace, and lines of operation in cyberspace. A specific discussion on the interplay between Department of Defense information network and defensive cyberspace operations will be presented to help define the operational areas of responsibility. This will be followed by a high level discussion on command and control within the cyberspace operational environment. Finally, recommended thoughts for addressing the two distinct aspects of operations on the cyberspace environment and operations in the cyberspace environment will be presented as part of the conclusion.

Framing the Environment

Cyberspace security and cyberspace defense rated so high for the Obama administration that only 4 months into office President Obama released a press statement on securing our nations cyber infrastructure.[2] Since this time, Department of Defense (DoD) have seen the birth of a new sub-unified command, United States Cyber Command (USCYBERCOM).[3] The world has also witnessed cyber used as a destructive weapon. The Iran nuclear program of 2010[4], Saudi Arabia oil company (Aramco) of 2012[5], and South Korea banking of 2013[6] cyber attacks are examples of cyberspace weapons used for destruction. Every modern nation around the world is raising the red flag on cyber espionage.[7] As a global leader, the United States has just recently released a policy stance towards specific cyberspace actions.[8] The United States government (USG) along with DoD is living through the maturation process of the cyberspace domain which presents and on occasion requires change. The nation is benefitting from the great promises as well as starting to understand and address the great perils of cyberspace.

The great promises in cyberspace started when the dot-com era took off through the 1990s. Innovations from entrepreneurs dominated the economic markets. The birth of new social mediums such as email, chat, and facebook connected nations and people around the world. Every person became a prospective news reporter linking local news to global news. Local domestic markets now had an easier means and capability to enter the global market. Industry now had greater access to resources such as raw materials, labor, and parts. The access, spread, and dissemination of information began to alter business, social, and nation-state norms.

The great perils arose when hostile and criminal actors began to adapt to the change in global norms. The increased capability to access, spread, and disseminate information enabled globalization of criminal activities, diverse ideologies, and corporate or nation-state espionage. The Mandiant APT1 Report of 2013 provides an outstanding example of nefarious activities attributed to a nation-state.[9]

How does DoD address the perils or more accurately the threats that create the perils? Addressing the perils to and in cyberspace is much like how the nation addressed and addresses people and property moving through any other domains. The perils require being addressed by international and domestic laws, policies, standards, and enforcement. There are laws, policies, and methods of enforcement for movement of personnel and property within the land, air, and maritime domains. Personnel and property are forms of payload carried by motor-vehicles, airplanes, and ships. Therefore, the same laws and policies should apply to cyberspace payloads for intellectual property, e-commerce, and e-banking. In June of 2013, the United States and 15 other countries signed a United Nations agreement that current international law will be applied and abided to within cyberspace.[10] This is the first step to enable legitimate and expeditious execution of legal and military actions as extensions of the U.S. National Security Diplomacy. United States policy makers, to include President Obama, have begun establishing the second step by announcing the United States policy stance on cyber espionage, theft, and attacks.[11] These announcements on establishing the national policy include speeches and press releases. Developing an enforcement capability through the U.S. Cyber Command approved force development model is a critical third step in advancing the cyberspace domain to a level on par with the other domains for conducting military operations.

What are the threats and how do cyber threats compare with other national threat priorities? The March 2013 Director of National Intelligence Worldwide Threat Assessment listed cyber threats as the number one threat to national security above terrorism, transnational organized crime, and weapons of mass destruction proliferation.[12] Cyber threats are defined as cyber attacks and cyber espionage in this document. A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate.[13] Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information.[14] The four categories of risk in cyberspace were listed as: increased risk to U.S. critical infrastructure, eroding U.S. economic and national security, information control and internet governance, and other actors including terrorist groups, hacktivists, and cyber criminals.[15] Eroding the United States economic and national security is the Obama administration's highest level cyberspace threat category as addressed during the China U.S. summit in June of 2013.[16]

Linking Doctrine

Cyberspace is a sub-set of the information environment. Joint Publication 3-12 identifies three dimensions of information environment: physical, informational, and cognitive. The physical dimension is composed of the command and control systems, decision makers, and support infrastructure that enable individuals or organizations to conduct operations.[17] The informational dimension is a place where information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, respond to, or act on information.[18]

The cognitive dimension has no physical or logical state that can be touched or viewed, unlike the other two dimensions. The cognitive dimension refers to the mental activities such as thinking, understanding, learning, and remembering.[19] The informational dimension is physical, logical, or both. Therefore, information can be touched or viewed. Information is a representation of linked, grouped, or analyzed data artifacts. Webster's dictionary defines information as knowledge obtained about someone or something and a fact or detail about a subject.[20] The physical dimension as defined in joint publication 3-12 must include both the physical and logical. Logical is defined as agreeing with the rules of logic.[21] In this case, the rules of logic are applied from a physical environment which provides an abstract representation of the physical state or element. Current support infrastructure and many command and control systems employ logical networks, logical meeting environments, and logical infrastructure components within the physical environment. Examples of logical infrastructure are virtual private networks, Microsoft Meeting Place, and virtual routers, virtual firewalls, and virtual servers respectively.

The three layers of cyberspace are the physical, logical, and persona. The three layers of cyberspace reside within the physical and informational dimensions of the information environment.[22] The cognitive dimension is more closely associated with the "Human Domain" and is not addressed in this paper. Refer to the Information Operations or Special Operation Forces Human Domain for further explanation or understanding of the cognitive dimension.[23] The physical network includes all the physical components to create and access the cyberspace environment. For example, physical network components may include wires, cables, radio frequencies, routers, servers, computers, radars, weapons systems, telecommunications systems, personal digital assistants, and other networked devices where data is created, manipulated, processed and stored. The logical layer is an abstract representation of the physical network. For example, a webpage appears with information that may actually contain information pulled from 2 to 250 physical servers. Another example, the phone service appears to connect directly with the phone switch but may actually be connected through a 100 switches. The third example would be all virtual devices or virtual networks. The persona layer is an abstraction of the logical network and consists of the people who actually use the network. Therefore, a persona must have one or more identities that can be identified, attributed, and acted upon. These identities may include e-mail addresses, social networking identities, other web forum identities, computer internet protocol addresses, and cell phone numbers.[24]

Three types of operations are conducted within the cyberspace environment: Department of Defense information network operations (DoDIN), defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).[25] Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[26] Department of Defense information network operations are operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks.[27] Defensive cyberspace operations is passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.[28] Offensive cyberspace operations are operations intended to project power by the application of force in or through cyberspace.[29]

Army Field Manual 3-38 discusses DoDIN operations as three types including network operations, network transport, and information services. Air Force Policy Directive 10-17 lists Air Force Information Network operations as Command, control, implement, configure, secure, operate, maintain, sustain, and defend. U.S. Cyber Command executes DoDIN operations as assigned to USSTRATCOM consisting of securing, operating, and defending. U.S. Cyber Command DoDIN operations are mostly discussed as DoD network operations and defending as defensive cyberspace operations.[30] DISA's Operations Directorate discusses support to U.S. Cyber Command for DoDIN operation and defense including execution of defensive cyberspace operations.[31] As each DoD organization continues to mature cyberspace at different rates the understanding and defining of the cyberspace lines of operation are not tightly synchronized. This loose synchronization and disparate maturity process induces large amounts of friction between Service and Department cylinders of excellence within the cyberspace domain. The friction even induces a fragmented lexicon within the community as just noted with naming and definitions of the DoDIN operations.

U.S. Cyber Command has identified and is promoting active defensive cyber operations as DCO response actions and passive defensive cyber operations as internal defensive measures[32]. Not all Service and Agency publications have been updated to reflect this lexicon change nor does it appear they all have agreement on the

DCO action terms. The two distinct DCO actions have been defined in two separate doctrine publications. A defensive cyberspace operation response action is a deliberate, authorized defensive measure or activity taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems.[33] Internal defensive measures are those defensive cyberspace operations that are conducted within the DODIN.[34]

Cyberspace is a man-made domain that resides in the information environment and interacts with all other warfighting domains. The information environment dimensions from Joint Publication 3-12 are paired to the cyberspace line-of-operations in the following ways. Department of Defense information network operations is the line of operation that creates, cares, and feeds the physical and logical devices and materials that make-up this domain. The DoDIN operations are executed in the physical dimension of the information environment. Defensive cyberspace operations is the line of operation that protects both the physical and logical aspects of this domain. DCO are executed in both the physical and informational dimensions of the information environment. Offensive cyberspace operations is the line of operation that projects force and influence on all three layers (physical, logical, and persona) of cyberspace. OCO are executed in all three dimensions (physical, informational, and cognitive) of the information environment.

DoDIN and DCO Interplay

Figure 1 provides a good visual diagram for continued discussion on the ownership and responsibilities of a mission or action executed along the seams. Mission responsibilities during an active or a live operation are not clearly defined. What entity has configuration change management authority and access to the physical and logical infrastructure for an in-progress defensive cyberspace action? What entity leads routine sustainment actions when an adversary covert operation is on-going? Figure 1 shows that both cyberspace attack and DCO response actions (DCO-RA) affect the whole cyberspace environment and activities. The figure also points out that DCO internal defensive measures (DCO-IDM) are explicitly linked between DCO and DoDIN operations. The figure reflects what most understand as traditional communications and information management as DoDIN operations. What the figure and most articles and directives do not address is the relationship and overlap of the three lines of operation, DoDIN, DCO, and OCO.

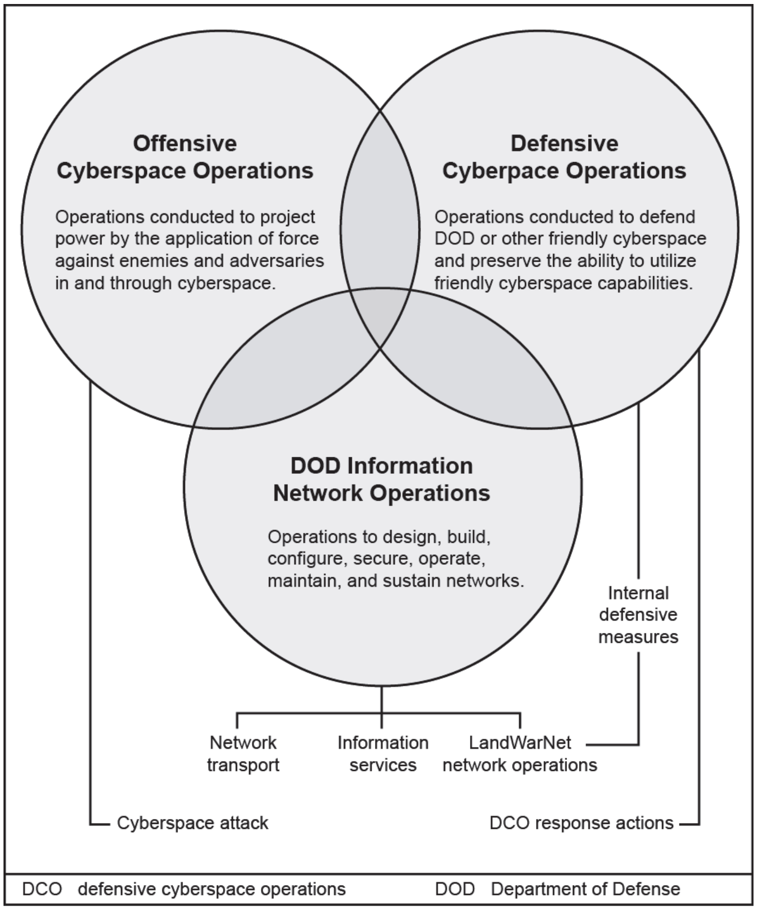

Offensive Cyberspace Operations
Operations conducted to project power by the application of force against enemies and adversaries in and through cyberspace.
Defensive Cyberpace Operations
Operations conducted to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.
DOD Information Network Operations
Operations to design, build, configure, secure, operate, maintain, and sustain networks.
Internal defensive measures
Network transport
Information services
LandWarNet network operations
Cyberspace attack
DCO response actions
DCO defensive cyberspace operations
DOD Department of Defense

Figure 1: Three Interdependent Functions[35]

Traditional terms grown out of the age of Net-Centricity such as Defense Information Systems Network (DISN), network defense, computer network defense response actions, information assurance, network assurance, and computer defense operations do not neatly translate into, if they fit at all, the updated lexicon of DoDIN, DCO, and OCO. Traditional information assurance and computer network defense make up two of those areas that quite frequently overlap with DoDIN operations and defensive cyber operations. Information assurance is an action that protects and defends information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.[36] Computer network defense is an action taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.[37] Network assurance is a transitional term used before DoDIN, DCO, and OCO lines of operation. Network assurance is a term that should no longer be used but is defined to include information assurance, computer network defense (including computer network defense response actions), and critical infrastructure protection in defense of the defense information systems network (DISN).[38] Computer network defense response actions (CND-RA) are actions that are preplanned in response to a known activity within the DISN. Defensive cyberspace operations-response actions (DCO-RA) are response actions taken outside the DoDIN as defined previously. Therefore, CND-RA and DCO-RA are not interchangeable nor do they overlap. Net assurance, computer net defense, and defense information systems network are all terms that have been superseded. The new terms of DCO-RA, DCO-IDM, and DoDIN are not direct substitutes.

Information assurance in its basic or simplistic form breaks down to credentials and access privileges that protect a cyberspace resource. The credentials and access privileges are what enable the different protection levels. These different protection levels may be applied to data, information stores, systems, or transport which implements varying degrees of availability, integrity, authentication, confidentiality, and non-repudiation. Computer network defense is fundamentally about responding to abnormal activity. DCO-IDM encompasses both information assurance and computer network defense measures. Abnormal activity could be an attempted access to a cyberspace resource with incorrect privileges or an increase in a system processor usage. Other abnormal activity would be the temporary loss of a resource or change in a resource configuration without prior approval or authorization. Each of these examples could be linked to an insider threat either physical, a person walking around, or logical, an adversary persona moving around inside the local cyberspace area. What immediate actions should be taken? What organization establishes the investigation and surveillance?

The military police's criminal investigations division is the most likely first organization contacted if the insider threat is perceived as a physical threat. The organization's security officer, local administrator, or servicing computer or network operation center is the most likely person or organization contacted if the insider threat is perceived as inside the network or a logical persona. The military police organization has the capability to establish surveillance, question possible observers or witnesses, review any access records, and detain or remove the threat.[39] What organizations have the capability or authority to execute like functions for a logical persona?

Department of Defense information network operations, as stated earlier, is to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. Remembering that a defensive cyberspace operation is defined as passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems, who has lead? The items in these definitions that create tension between DoDIN operations and defensive cyberspace operations communities are “configure, secure, and preserve information assurance” when balanced against “preserve and protect data, networks, and net-centric capabilities”. The term “Secure” is defined as protecting or providing protection from danger or harm or guard so that no one can enter or leave without approval.[40] Referring back to the example of the insider threat of abnormal activity by a logical persona, which cyber operational community has responsibility? Both, the DoDIN and DCO communities have a shared responsibility. The DCO community should have lead.

Defining Operational Space

Why should the defensive cyberspace operations community have lead for resolving the insider threat of abnormal activity by a logical persona? Both communities will have similar if not identical training backgrounds. But, each community has a different focus for applying the training. Defensive cyberspace operations are focused on the defense against the adversary’s objectives or ends and the concepts or ways to achieve them. DCO is adversary threat focused. This community tracks the employment of tactics and techniques employed by the adversary to achieve their objectives to include the employment of a new weapon. Department of Defense information network operations are focused on cyberspace environment sustainment and defense against the known attack weapons or the adversary’s means. Sustainment would include actions to prevent or correct a maintenance failure, loss of access to a resource, or a degraded service.[41] An attack weapon would be a SQL injection, Trojan horse, or multiple request actions (a denial of service). DoDIN employs friendly tactics and techniques to block and tackle the adversary’s weapon of choice and sustainment failures.

Department of Defense information network operations are first and foremost the physical sustainment and maintenance of the cyberspace environment. DoDIN must retain configuration management control of all devices physical and logical in-order to maintain the cyberspace environment availability for required daily business operations and for support to the other four domain operations. As a combat maneuver domain, both DCO and OCO require a form of configuration management control to remove or employ obstacles as part of battlespace preparation or maneuver support.

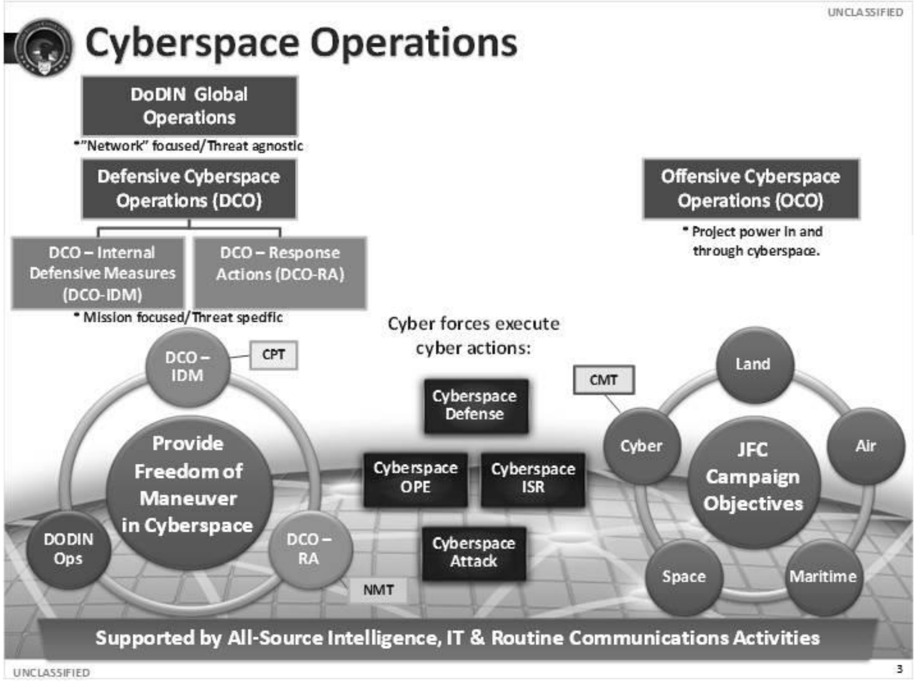
Defensive cyberspace operations are first and foremost focused on the adversary actions and movements inside the cyberspace environment. Once the adversary begins execution of an event or attack, the cyberspace action executes at net-speed. The DCO community must have a form of configuration management control or authority in-order to stop or slow the adversary’s actions in cyberspace. Since the cyberspace environment is man-made, the capability to change the local or global environment is instantaneous with a configuration change of the physical or logical device. A single configuration change like turning off TCP/IP in the cyberspace domain could have the same effect as removing the oceans from the maritime domain.

Therefore, configuration management is of upmost importance to avert a cyberspace disaster or negative consequences on the cyberspace environment.

The defensive cyberspace operational community will lead the resolution of abnormal activity generated by a logical persona since that community is adversary threat focused. The DCO community will either understand or identify the adversary's objectives and ways to attempt achievement of those objectives. The DoDIN community will support by providing information and configuration change management actions in support of the DCO community. The DoDIN operational community will implement the modifications to the configuration management of the physical and logical devices in-order to alert, indentify, deny, or implement other actions as directed by the DCO community. The same indicators and warnings (events and alerts) may drive different assessments by each community based on their different focus. The indication of an overheating processor is a DoDIN indication of a cooling system failure or an over taxed device that required rerouting traffic to maintain availability of other cyberspace resources. The same overheating processor is a DCO indication of illicit activity or deception to force traffic to reroute in favor of an adversary action. The DCO community would intervene into the DoDIN operations if this activity was identified or previously known as an adversary's tactic. A post mortem investigation will determine if the overheating processor was in-fact a nefarious act or mechanical sustainment issue.

Several questions posed earlier in this paper were not answered. The discussion above helps to delineate interaction between the roles and responsibilities of DoDIN and defensive cyberspace operations. First, what entity has configuration change management authority and access of the physical and logical infrastructure for an in-progress defensive cyberspace action? The authority to physically change the configuration is the DoDIN operators. The DCO teams have authority to direct or recommend changes to be implemented based on threat. Second, what entity leads routine sustainment actions when an adversary covert operation is on-going? When the DCO teams are monitoring or reacting to a covert action, the DCO teams must inform and advise the DoDIN teams to avoid fratricide or lost target acquisition. Third, what organizations have the surveillance capability or authority to execute like functions for a logical persona? The DCO teams have the capability and can obtain the authority to execute surveillance like activities, title 18 or title 50 as required, within the DoDIN for suspected adversary activity. Surveillance activities outside the DoDIN are a separate discussion on authorities not addressed in this paper.

Cyber is the fifth domain utilized to project United States policy and power. Figure 2 is U.S. Cyber Command's cyberspace line of operations briefing slide.[42] U.S. Cyber Command identifies defensive cyberspace operations as focused on threat specific actions. Department of Defense information network operations are identified as focused on threat agnostic activities. This links to the earlier discussion that DoDIN defensive operations are defense against a specific cyber weapon not the tactics or method of employment. This figure also re-enforces the DCO discussion about DCO being adversary threat focused. Freedom of maneuver in cyberspace is all based on configuration management since it is a man-made environment. DCO identifies and recommends or directs DoDIN configuration management changes to enable friendly and deny adversary freedom of maneuver within the DoDIN. DCO teams recommend defensive cyberspace operations response actions for approval to enable friendly force freedom of maneuver in neutral or adversary cyberspace. DCO teams will also recommend defensive cyberspace operations response actions for approval to deny adversary freedom of maneuver in friendly or neutral cyberspace.



UNCLASSIFIED

Cyberspace Operations

DoDIN Global Operations

*"Network" focused/Threat agnostic

Defensive Cyberspace Operations (DCO)

DCO – Internal Defensive Measures (DCO-IDM)

DCO – Response Actions (DCO-RA)

* Mission focused/Threat specific

Offensive Cyberspace Operations (OCO)

* Project power in and through cyberspace.

Cyber forces execute cyber actions:

Cyberspace Defense

Cyberspace OPE

Cyberspace ISR

Cyberspace Attack

DCO – IDM

CPT

Provide Freedom of Maneuver in Cyberspace

DODIN Ops

DCO – RA

NMT

CMT

Land

Cyber

JFC Campaign Objectives

Air

Space

Maritime

Supported by All-Source Intelligence, IT & Routine Communications Activities

UNCLASSIFIED

3

Figure 2: USCYBERCOM Lines of Operation[43]

There is another telling story about figure 2. Cyber force execute actions are defense, operational preparation of the environment, attack, and intelligence, surveillance, and reconnaissance. There is no reference of execution to sustain, build, secure, or maintain cyberspace; DoDIN operations. The only reference is supported by information technology and routine communications activities along the bottom of the slide. This reduced emphasis on DoDIN operations links the discussion about requiring two distinct communities to focus on the two aspects of the domain. One aspect of build and sustain and the other aspect of combat operations in and through. To project power in cyberspace or to treat the cyberspace domain as a warfighting domain, forces must be trained, equipped, and apportioned to execute combat operations in and through the domain just as forces are trained, equipped, and apportioned in the land, air, space, and maritime domains. Projecting power is not a static defense.

Command and Control

The Secretary of Defense approved the implementation of the Transitional Cyberspace Command and Control model in May of 2012.[44] The transitional cyberspace command and control model reflects the cyberspace lines of operation and missions arrayed across the cyberspace force structure. Cyber mission teams conduct operations outside the DoDIN infrastructure functions and mission. The cyber protection platoons conduct defensive functions, missions, and operations inside the DoDIN infrastructure. The joint information environment operation centers and the Service network operation security centers execute DoDIN operations. The Joint Information Environment (JIE) end-state is a secure environment, comprised of shared IT infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize IT efficiencies.[45] The joint information environment end-state identifies that this is an initiative within the DoDIN. The JIE will drive change within the DoDIN but will not drive any changes that affect the discussions in this paper. Services and DISA will still be maintaining infrastructure and information services as part of the DoDIN.

The integration of DCO and DoDIN operations currently occurs at the U.S. Cyber Command joint operations center, the Combatant Command joint cyber center or the joint cyber component command, and the Defense Information Systems Agency command center. Understanding the mission focus as described previously in this paper, this model outlines the integration points and retains execution control under the current DoDIN and DCO mission owners. Command and control relationship lines of the transitional cyberspace command and control model will change or morph as the cyberspace domain continues to mature in both capabilities of the workforce and tools. The commands and centers are not likely to change even if the U.S. Cyber Command is promoted to a full Unified Command or Service.

Who is best equipped or should maintain responsibility to train cyber forces? Discussions at all levels of Department of Defense are occurring on this topic. Some thoughts circling around about cyber force structure are to make cyberspace a separate Service, make cyberspace a Unified Command, or remain a Sub-Unified Command with greater Service obligations. Each thought has a laundry list of positives and negatives. The fact that remains is that cyberspace has elevated or matured to a point that it ranks as the number one national security threat. U.S. Special Operations Command (USSOCOM) is a Unified Command that addresses unconventional and asymmetric threat forces. USSOCOM was established to address the United States number one security threats of the past quarter of a century which were terrorism, transnational and weapons of mass destruction proliferation through unconventional warfare. USSOCOM is delegated limited budget, training, and doctrine authorities to address the unconventional and asymmetric threats.[46] Cyberspace direct actions require a unique specialized platform and tools. The training is highly specialized and low density. Doctrine is specific to the skills and missions. Therefore, the specialized doctrine is not applicable to the conventional cyber force.[47] The maturation of the cyber force and continued sustained threat will soon if not already surpass the limitations of the current command and control structure as a Sub-Unified Command. A critical decision point will arrive once the cyber forces have matured in doctrine and capability to a point that the

National Security Agency assets are not required to enable combat missions in the cyberspace domain.

Cyberspace still has two distinct training and doctrine aspects. The first aspects are the cyberspace combat support and service support functions to establish the domain, maintain the domain, and support operation in the domain. The support and service support functions include the building, sustaining, and securing the physical environment to establish the domain. The second aspect is the combat operations that take place inside the cyberspace domain. The Services and Defense Information Systems Agency have well established operating and training doctrine to execute DoDIN operations. Understanding that it is a Service mission to present trained forces to the joint commander, Special Operations Command executes missions globally for the joint force commander. It may serve the Department of Defense to continue execution of all cyberspace missions outside the DoDIN under one provider just as USSOCOM executes for unconventional and asymmetric missions as one provider.[48] The Services only provide support to and protection for special operations forces. The Special Operations Forces current model for the recruiting, specialized training, and service obligation process would make a good model for U.S. Cyber Command if promoted to a unified command with appropriate authorities to execute. This would relieve each Service from establishing advanced cyber combat training.[49] Services will still be obligated to train and present forces but at a lower level of expertise and on a specific sub-set of skills. This will enable operational support of and protection for the specialized cyber direct action or reconnaissance teams.

Conclusion and Recommendation

The cyber threats including cyber attacks and cyber espionage are identified as the number one threat to the United Sates National Security. To address and mitigate the threat to the U.S. National Security, the policies, laws, and standards must be in place. Operating in the cyberspace domain is no different than operating in the land, air, maritime, or space domains. DoD must establish a capable and creditable cyberspace combat force to enforce the nations policies and laws when called upon to do so within the cyberspace domain. DoD must also ensure resiliency of the cyberspace environment in-order to continue business operations in support of all five domains. To that end, much work is still required to address the passage of lines and rear area defense operations within the cyberspace domain between the cyberspace combat force and the cyberspace support forces. The Services and DISA are slow to embrace the maturation of the cyberspace domain and relinquish overlapping mission space from previous net-centricity doctrine to current doctrine for DCO to USCYBERCOM. This paper addressed some confusion in terminology and mission space between DCO and DoDIN operations as the cyberspace domain continues to mature.

The cyberspace domain requires a distinctly separate community that focuses on the cyber infrastructure which includes both the physical and logical cyberspace resources. This community executes the DoDIN line of operations. The Services and DISA have this line of operation well established and should continue to retain. The second community focuses on the cyberspace combat operations in and through but not on the cyberspace domain. This community executes the DCO and OCO lines of operation. U.S. Cyber Command has these roles and continues to mature. The two communities must be tightly linked to prevent opening seams for an adversary to exploit. The cyberspace command and control structure must maintain a single top level command that maintains overall authority of both the two distinct communities. The purpose of a single authority is to prevent or mitigate seams between the two community's missions. The current approved Transitional Cyber C2 Model provides for this if the Service and DISA would implement as intended. The mortar in DoD's cyberforce firewall to protect and defend the United States National Security is the combination of both the cyberspace resiliency (provide by DoDIN OPS) and a capable and creditable cyber combat force (DCO and OCO).

Endnotes

[1] Barack Obama, "Remarks by President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed March 12, 2014).

[2] Ibid.

[3] "DoD Announces First USCYBERCOM and First USCYBERCOM Commander,"*U.S. Department of Defense News Release,* May 21, 2010, http://www.defense.gov/releases/release.aspx?releaseid=13551 (accessed March 14, 2014).

[4] Michael Gross, "A Declaration of Cyber-War," *Vanity Fair Online*, April 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (accessed March 21, 2014).

[5] Reuters, "Aramco Says Cyberattack was Aimed at Production," *The New York Times Online*, December 9, 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0 (accessed March 21, 2014).

[6] Choe Sang-Hun, "Computer Networks in South Korea are Paralyzed in Cyberattacks," *The New York Times Online*, March 20, 2013, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all (accessed March 21, 2014).

[7] Tobias Feakin, "Enter the Cyber Dragon: Understanding Chinese Intelligence Agencies' Cyber Capabilities," *ASPI,* no. 50 (June 2013): 6.

[8] Philip Rucher, "Obama Warns Xi that Continued Cybertheft Would Damage Relations," *The Washington Post Online*, June 9, 2013, http://www.washingtonpost.com/politics/obama-warns-xi-that-continued-cybertheft-would-damage-relations-us-officials-said/2013/06/08/04843edc-d075-11e2-8845-d970ccb04497_story.html (accessed March 21, 2014).

[9] Dan Mcwhorter, "Mandiant Exposes APT1: Exposing One of China's Cyber Espionage Units," February 18, 2013, https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/ (accessed March 21, 2014).

[10] Detlev Wolter, "The UN Takes a Big Step Forward on Cybersecurity," *Arms Control Today*, September 2013, http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity (accessed March 6, 2014).

[11] Bill Gertz, "Rice Warns China to Curb Cyber Espionage," *The Washington Free Beacon*, November 21, 2013, http://freebeacon.com/rice-warns-china-to-curb-cyber-espionage/ (accessed March 19, 2014).

[12] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, (Washington, DC: Director of National Intelligence for Senate Select Committee on Intelligence March 12, 2013), 1.

[13] Ibid.

[14] Ibid.

[15] Ibid., 3.

[16] Scott Neuman, "Chinese Cyber Hacking Discussed at Oboma-Xi Summit," *NPR*, June 9, 2013.

[17] U.S. Joint Chiefs of Staff, *Joint Cyberspace Operations,* Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, February 2013).

[18] Ibid.

[19] Marriam Webster Dictionary, "Cognitive," http://www.merriam-webster.com/dictionary/cognitive (accessed March 14, 2014).

[20] Marriam Webster Dictionary, "Information," http://www.merriam-webster.com/dictionary/information (accessed March 30, 2014).

[21] Marriam Webster Dictionary, "Logical," http://www.merriam-webster.com/dictionary/logical (accessed March 14, 2014).

[22] U.S. Department of the Army, *Cyber Electromagnetic Activities,* Army Field Manual 3-38 (Washington, DC: U.S. Department of the Army, February 2014), 1-6.

[23] Claudette Roulo, "McRaven: Success in Human Domain Fundamental to Special Ops," *American Forces Press Service*, June 5, 2013, http://www.defense.gov/news/newsarticle.aspx?id=120219 (accessed March 19, 2014).

[24] U.S. Department of the Army, *Cyber Electromagnetic Activities*, 3-9.

[25] Ibid., 1-3.

[26] U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 2011).

[27] U.S. Joint Chiefs of Staff, *Joint Cyberspace Operations*.

[28] Ibid.

[29] Ibid.

[30] Cheryl Pellerin, “Cyber Command Adapts to understand Cyber Battlespace,” *American Forces Press Service*, March 7, 2013.

[31] *Defense Information System Agency Operation Directorate Home Page*, http://www.disa.mil/About/Our-Organization-Structure/OD-HQ (accessed March 18, 2014).

[32] Maj Gen Brett T. Williams, “Cyberspace Operations,” briefing slides, Carlisle Barracks, PA, U.S. Army War College, March 4 2014.

[33] U.S. Joint Chiefs of Staff, *Joint Cyberspace Operations*.

[34] U.S. Department of the Army, *Cyber Electromagnetic Activities*, 3-6.

[35] Ibid., 3-2.

[36] U.S. Joint Chiefs of Staff, *Joint Cyberspace Operations*.

[37] U.S. Joint Chiefs of Staff, *Joint Communication Systems,* Joint Publication 6-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 2010).

[38] John G. Grimes, *Department of Defense NetOps Strategic Vision* (Washington, DC: U.S. Department of Defense Chief Information Officer, December 2008), 2.

[39] U.S. Department of the Army*, Military Police Operations,* Army Field Manual 3-39 (Washington, DC: U.S. Department of the Army, August 2013), 3-1.

[40] Marriam Webster Dictionary, “Secure,” http://www.merriam-webster.com/dictionary/secure (accessed March 16, 2014).

[41] U.S. Department of the Army, *Signal Support to Operations*, Army Field Manual 6-02 (Washington, DC: U.S. Department of the Army, January 2014), 1-7.

[42] Williams, “Cyberspace Operations.”

[43] Ibid.

[44] Zachary Fryer-Biggs, “Penetta Green Lights First Cyber Operations Plan,” *Defense News*, June 6, 2012, http://www.defensenews.com/article/20120606/DEFREG02/306060010/Panetta-Green-Lights-First-Cyber-Operations-Plan (accessed March 18, 2014).

[45] DISA Mission Partners Conference, “DoD ESI & Joint Information Environment,” May 7, 2012, Slide 11, http://www.disa.mil/News/Conferences-and-Events/DISA-Mission-Partner-Conference-2012/~/media/Files/DISA/News/Conference/2012/DoD_ESI_JIE.pdf (accessed March 18, 2014).

[46] *U.S. Special Operations Command Home Page*, http://www.socom.mil/Pages/AboutUSSOCOM.aspx (accessed March 18, 2014).

[47] James Stavridis and David Weinstein, “Time for a U.S. Cyber Force,” *U.S. Naval Institute Proceedings Magazine* 140, no. 1 (January 2014): 331.

[48] Ibid.

[49] Ibid.