United States Army War College

Strategic Cyberspace Operations Guide

1 June 2016

CENTER for STRATEGIC LEADERSHIP CSL

Middle States Accreditation

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.

Disclaimer: The systems, processes, and views described in this guide reflect the judgment and interpretation of the editors, and does not necessarily represent the official policies or positions of the Headquarters, Department of the Army, the Department of Defense, or the United States Government.

The text is a synthesis and interpretation of existing National, Defense, Joint, and Service systems, processes, and procedures, and will be updated in accordance with changes in policy and doctrine.

This Page Intentionally Blank

Foreword

1. This publication provides a guide for U.S. Army War College students to understand design, planning, and execution of cyberspace operations at combatant commands (CCMDs), joint task forces (JTFs), and joint functional component commands. It combines existing U.S. Government **Unclassified** and "**Releasable to the Public**" documents into a single guide.

2. This strategic guide follows the operational design methodology and the joint operation planning process (JOPP) detailed in Joint Publication 5-0, *Joint Operation Planning* and applies these principles to the cyberspace domain found in Joint Publication 3-12(R), *Cyberspace Operations*. However, this publication is not to be cited, copied, or used in lieu of doctrine or other official publications.

The U.S. Army War College Strategic Cyberspace Operations Guide contains six chapters:

Chapter 1 provides an overview of cyberspace operations, operational design methodology, and joint planning, and execution.

Chapter 2 includes a review of operational design doctrine and applies these principles to the cyberspace domain.

Chapter 3 reviews the joint operation planning process and identifies cyberspace operations planning concerns.

Chapter 4 describes cyberspace operations during the execution of joint operations.

Chapter 5 provides an overview of cyberspace operations in the homeland.

Chapter 6 includes a case study on the Russian – Georgian conflict in 2008 with a focus on cyberspace operations.

Appendix A provides an overview of cyberspace strategies, guidance, and doctrine.

Appendix B includes a description of U.S. Government, Department of Defense, Joint, and Service cyberspace organizations.

3. This publication was compiled and edited by Mr. Benjamin Leitzel and Mr. Anthony Allard.

4. This document is based on U.S. policy and doctrine and will be updated on a routine basis to reflect changes in guidance. We encourage comments to improve this guide – send recommended changes to:

Center for Strategic Leadership
ATTN: Emerging Concepts and Doctrine Division
650 Wright Avenue
Carlisle, PA 17013

This Page Intentionally Blank

Table of Contents

Chapter 1: Introduction

"We ... need to develop a framework within which to deter cyber threats, and obviously attributing threats and managing escalation and hardening ourselves against cyberattacks are all areas that require more work"

General Joseph Dunford,
Chairman of the Joint Chiefs of Staff[1]

1. This guide follows the operational design methodology and the joint operation planning process (JOPP) and applies these principles to the cyberspace domain. Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[2] Commanders must develop the capability to direct operations in the cyber domain since strategic mission success increasingly depends on freedom of maneuver in cyberspace (see Figure 1-1).[3]

2. The President and the Secretary of Defense (SecDef) provide strategic guidance to the joint force. This guidance is the common thread that integrates and synchronizes the planning activities and operations. It provides purpose and focus to the planning for employment of military force.[4]

3. The commander and staff develop plans and orders through the application of the operational design methodology and by using JOPP. Operational design results in the commander's operational approach, which broadly describes the actions the joint force needs to take to reach the end state. The commander and staff translate the broad operational approach into detailed plans and orders using JOPP.[5] Planning continues during execution, with an initial emphasis on refining the existing plan and producing the operations order and refining the force flow utilizing employed assigned and allocated forces.[6]

4. Commanders integrate cyberspace capabilities at all levels and in all military operations. Plans should address how to effectively integrate cyberspace capabilities, counter an adversary's use of cyberspace, secure mission critical networks, operate in a degraded environment, efficiently use limited cyberspace assets, and consolidate operational requirements for cyberspace capabilities. While it is possible that some military objectives can be achieved by CO alone, CO capabilities should be integrated into the joint force commander's plan and synchronized with other operations during execution.[7]

Figure 1-1: Strategic Cyber Warfare

This Page Intentionally Blank

Chapter 2: Design

I. Operational Design

1. Joint Publication 5-0, *Joint Operation Planning*, describes operational design methodology and the joint operation planning process (JOPP). Operational design requires the commander to encourage discourse and leverage dialogue and collaboration to identify and solve complex, ill-defined problems. The operational approach is a commander's description of the broad actions the force must take to achieve the desired military end state. The operational approach is based largely on an understanding of the operational environment and the problem facing the commander. Once the commander approves the approach, it provides the basis for beginning, continuing, or completing detailed planning (see Figure 2-1).[8]

a. This methodology incorporates three distinct aspects to produce an operational approach. Together, they constitute an organizational learning methodology that corresponds to three basic questions that must be answered to produce an actionable operational approach to guide detailed planning:

(1) Understand the strategic direction. (What are the strategic goals to be achieved and the military objectives that support their attainment?)

(2) Understand the operational environment. (What is the larger context that will help me determine our problem?)

(3) Define the problem. (What problem is the design intended to solve?)

(4) The answers to these three questions support the development of an operational approach. (How will the problem be solved?)[9]

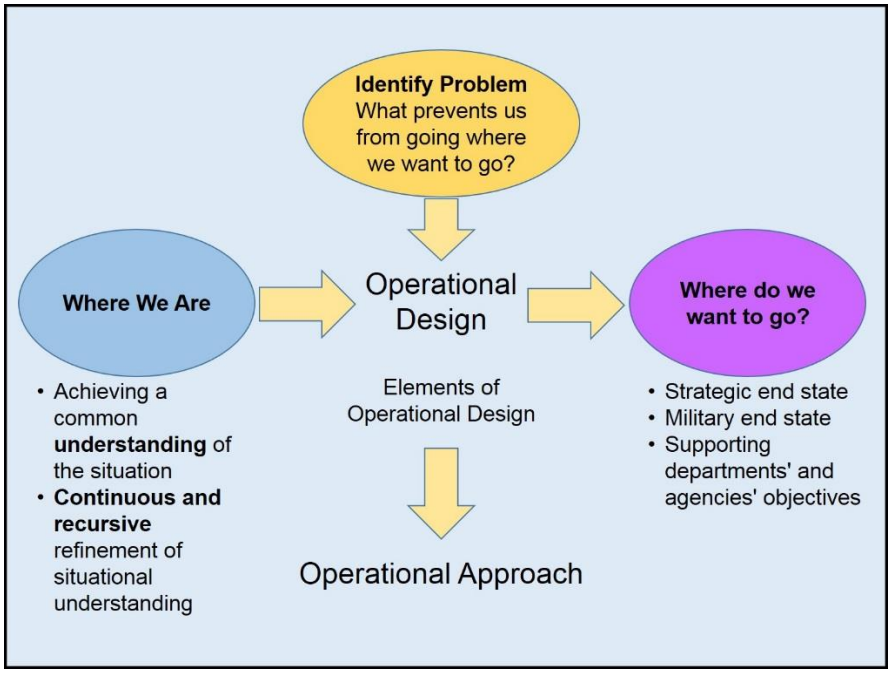

Figure 2-1: Developing the Operational Approach[10]

2. **Understand the Strategic Direction**. The President, Secretary of Defense (SecDef), Chairman of the Joint Chiefs of Staff (CJCS), and Combatant Commanders (CCDRs) all promulgate strategic guidance. In general, this guidance provides long-term as well as intermediate or ancillary objectives. It should define what constitutes "victory" or success (**ends**)

and allocate adequate forces and resources (**means**) to achieve strategic objectives. The operational approach (**ways**) of employing military capabilities to achieve the ends is for the supported commander to develop and propose. Connecting resources and tactical actions to strategic ends is the responsibility of the operational commander.[11]

3. **Understand the Operational Environment**. The operational environment is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors of the air, land, maritime, and space domains and the information environment (which includes cyberspace). Understanding the operational environment helps the commander to better identify the problem; anticipate potential outcomes; and understand the results of various friendly, adversary, and neutral actions and how these actions affect achieving the military end state.[12]

4. **Define the Problem**. Once armed with an initial understanding of the operational environment's current and desired systems, the design effort shifts to the challenge of understanding and describing the problem (those factors that must be addressed to change the current system to the desired system).[13]

> a. Defining the problem is essential to solving the problem. It involves understanding and isolating the root causes of the issue at hand—defining the essence of a complex, ill-defined problem. Defining the problem begins with a review of the tendencies and potentials of all the concerned actors and identifying tensions among the existing conditions and the desired end state. The problem statement articulates how the operational variables can be expected to resist or facilitate transformation and how inertia in the operational environment can be leveraged to ensure the desired conditions are achieved.[14]
>
> b. As the commander and staff gain an understanding of the problem within the context of the operational environment, potential solutions should become evident. The configuration of tensions, competition, opportunities, and challenges may reveal ways to interact with various aspects of the environment in order to transform it to the desired system. Analyzing these options often requires coupling potential actions to a problem by quickly wargaming their possible outcomes. This deepens understanding, informs the commander's ability to visualize friendly actions, and enables the commander to expedite detailed planning by developing intent and planning guidance.[15]

5. **Develop an Operational Approach**. The operational approach reflects understanding of the operational environment and the problem while describing the commander's visualization of a broad approach for achieving the desired end state. It is the commander's visualization of how the operation should transform current conditions into the desired conditions at end state – the way the commander wants the operational environment to look when operations conclude (see Figure 2-2).

> a. The operational approach is how the commander believes U.S. instruments of national power and other interorganizational actions should address the various factors that comprise the gap between the current and desired systems. The resulting product provides the foundation for the commander's planning guidance to the staff and collaboration with interorganizational partners. The commander and staff should continually review, update, and modify the approach throughout planning and execution as the operational environment, end state objectives, or the problem change.

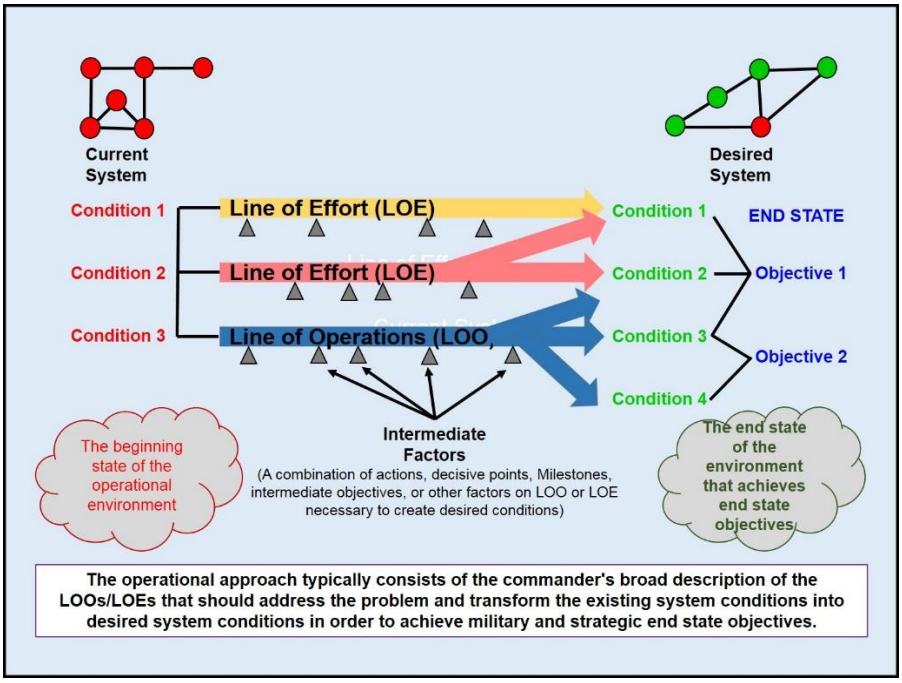

Figure 2-2: The Operational Approach[16]

b. In developing an appropriate operational approach, the commander should address the following questions:

(1) What are the strengths and weaknesses of the various actors?

(2) What are the opportunities and threats?

(3) How do we go from the existing conditions to the desired conditions?

(4) What will be the likely consequences as we seek to shape the operational environment toward a desired set of conditions?

c. The operational approach should describe the operational objectives that will enable achievement of the key conditions of the desired end state. The operational approach may be described using lines of operation (LOOs)/lines of effort (LOEs) to link decisive points to achievement of objectives. It should also include a description of how key adversarial desired conditions will be precluded, and how other non-adversarial desired conditions will be mitigated.

II. Strategic Direction and Cyberspace.

1. In 2012 President Obama directed the Department of Defense (DOD) to organize and plan to defend the nation against cyberattacks of significant consequence, in concert with other U.S. government agencies. In response, the DOD developed *Department of Defense Cyber Strategy* that focuses on three cyber missions (see Appendix A for cyberspace strategies, guidance, and doctrine):

a. defend DOD networks, systems, and information;

b. defend the United States and its interests against cyberattacks of significant consequence; and

c. provide integrated cyber capabilities to support military operations and contingency plans.[17]

III. Understanding the Cyberspace Environment.

1. **Introduction**. The ability to operate in cyberspace has emerged as a vital national security requirement. The growing impact of information warfare on military operations further increases the importance of cyberspace. As technological capabilities and instantaneous access to information continue to grow, the opportunities for real-time communication and information sharing expand. These capabilities are vital to economic and national development. However, reliance on these capabilities demands protection of the networks and information. Adversary activity in cyberspace could threaten the United States' dominance in the air, land, maritime, and space domains as they become increasingly interconnected and dependent on cyberspace technology.

a. **Cyberspace comprises the Internet, networks, systems, associated peripherals, data, and users** in the information environment. This interconnected environment is important to global governance, commercial, military, and national security. A major challenge for the United States and its allies is protecting and defending the environment from adversaries. The host of cyberspace adversaries and threats include state actors, non-state actors, criminal organizations, general users, rogue individual hackers, and, in many cases, internal personnel. Conversely, many of these threats may also be vulnerable through cyberspace.[18]

b. The **Department of Defense information networks (DODIN)** are a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.[19]

2. **Unique Cyberspace Capabilities and Characteristics**. Cyberspace is a global enabler for expedient, dynamic information exchange impacting all aspects of life. It allows instantaneous information flow across the globe for financial transactions as well as the movement and tracking of products and goods. However, it also allows adversaries to access this information and disrupt vital operations from any location. Cyberspace is difficult to regulate due to ease of accessibility. From a military perspective, cyberspace activities rarely require movement of forces, allowing engagement from extended stand-off ranges. It also enables the influence of populations that are inaccessible through the other domains.

a. **Can be reverse engineered**: Unlike munitions, which are normally destroyed upon use, cyberspace activities include code that can be saved, analyzed, and recoded for use against allies or friendly nations. Planners must account for the possibility of a "cyber ricochet"[20] in which cyber activities are turned against the originator or other unintended through reverse engineering.

b. **No Single National/International Ownership**: While someone owns each physical component of cyberspace, the whole of cyberspace is not under any single nations' or entities' complete control. The infrastructure is a disparate combination of public and private networks without standardized security or access controls. This arrangement enables free information flow, but the lack of controls hinders global accountability, standardization, and security. The traditional concept of and territorial integrity can be unclear due to the nature of cyberspace.

c. **Lack of Cooperation/Collaboration**: The lack of international laws and regulations governing the environment complicates responses to actions in this domain. The difficulty in tracing the source of a cyberattack makes them easily deniable, especially if

conducted by individual "hackers." Further hindering collaboration is the tendency to deny that a cyberspace attack has occurred to prevent loss of trust in an organization's cyber security measures.

d. **Low Cost**: Cyberspace is the most affordable domain through which to attack the United States. Viruses, malicious code, and training are readily available over the Internet at no cost. Adversaries can develop, edit, and reuse current tools for network attacks. Inexpensive tools and training allow an adversary to compete without costly ships, aircraft, or missiles. Furthermore, an adversary can impose significant financial burdens on nations that rely heavily on cyberspace by forcing them to invest in cyberspace defense. Currently, "military-grade" cyberspace capabilities remain too expensive for most malign actors, but they can buy relatively inexpensive services of professional hackers.

e. **Volatile***:* Successful cyberspace attacks depend on vulnerabilities within the adversary's network. Identifying these vulnerabilities and creating cyberspace capabilities sometimes require great expense. If an adversary discovers the targeted network's vulnerability and closes it, the cyberspace attack technique is rendered immediately and unexpectedly useless despite the development expense. For this reason, great care must be taken to prevent alerting adversaries to vulnerabilities in their networks.

f. **Speed**: Cyberspace operations occur quickly. However, preparation for those operations is often extensive. An intense study of the adversary's network may be required to learn system specifications and understand patterns of life. Therefore, a cyberspace unit operating on one adversary's networks may not be able to shift focus to another target without substantial preparation.

g. **Unintentional cascading effects**: Another unique characteristic of cyberspace is the potential for unintended cascading effects. Capabilities and munitions in the natural domains lose momentum the greater distance from impact. However, physical distance means very little in cyberspace. While cyberspace capabilities are developed and evaluated in computer labs and cyberspace ranges, there can never be complete assurances as to how a capability will behave or where it might spread when introduced to the great expanse of cyberspace.

h. **Layers**: Cyberspace can be visualized as three layers: Physical Network, Logical Network, and Cyber - Persona (see Figure 2-3). Adversaries might attack any of these layers to disrupt, degrade, or destroy cyberspace capability. Conversely, each of these layers presents a means to attack adversaries' use of cyberspace.

- The **physical layer** includes all hardware assets – computers, servers, routers, satellite links, etc. – enabling the movement of information in and through cyberspace. Related to the physical layer is cyberspace's reliance on the electromagnetic spectrum (EMS), where much of cyberspace's code moves and is, therefore, vulnerable to jamming or manipulation.
- The **logical layer** is the abstract portion of the physical layer. This layer reflects information represented and accessible in multiple locations through Internet Protocol and uniform resource locator (URLs).
- The **cyber-persona** layer is an extension of the logical layer and represents the users, entities, and organizations on the network. This layer applies the same rules that govern the logical layer.[21]

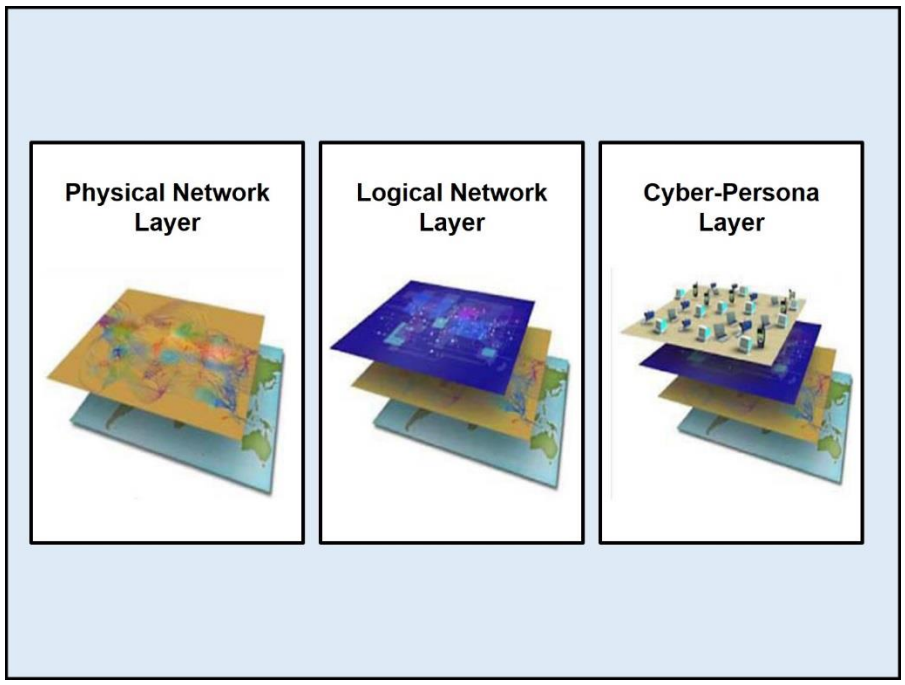

Figure 2-3. The Three Layers of Cyberspace[22]

3. **Intelligence Support**. The intelligence team provides critical insights to help the commander and staff understand the cyberspace environment. They draw on intelligence products focused on vulnerabilities and threats in the cyberspace domain. The assessment of enemy cyberspace capabilities, to include an examination of doctrinal principles and tactics, techniques, and procedures (TTP), and observed patterns of enemy operations in the cyberspace domain lead to a determination of possible enemy courses of action (COAs).[23]

IV. Defining the Problem: Threats and Challenges in Cyberspace.

1. The commander faces a unique set of cyberspace threats and challenges while conducting operations in a complex global security environment.

2. **Cyber Threats**. Cyberspace presents the commander with many threats ranging from nation states to individual actors.

a. **Key Cyber Threats**. From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of 11 September 2001. Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. Actors may penetrate U.S. networks and systems for a variety of reasons, such as to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives. These threats can be internal or external to cyberspace (see Figure 2-4).

b. Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property from global

businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.

c. In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.[24]

(1) **Nation State Threat**. This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Other nations may employ cyberspace to either attack or conduct espionage against the U.S. Nation state threats involve traditional adversaries and sometimes, in the case of espionage, even traditional allies. Nation states may conduct operations directly or may outsource them to third parties to achieve their goals.

(2) **Transnational Actor Threat**. Transnational actors are formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist actions within cyberspace.

(3) **Criminal Organization Threat**. Criminal organizations may be national or transnational in nature. Criminal organizations steal information for their own use or, in turn, to sell to raise capital. They also may be used as surrogates by nation states or transnational actors to conduct attacks or espionage through CO.

(4) **Individual Actors or Small Group Threat**. Individual actors or small groups of people can illegally disrupt or gain access to networks or computer systems. Their intentions are as varied as the number of groups and individuals. These actors gain access into systems to discover vulnerabilities, sometimes sharing the information with the owners; however, they also may have malicious intent. Political motivations often drive their operations, and they use cyberspace to spread their message. They may also create and then install malware on commercial or government systems. These actors can be exploited by others, such as criminal organizations or nation states, in order to execute concealed operations against targets in order to preserve their identity or create plausible deniability.[25]

(5) **Insider Threat**. The "insider" is an individual currently or at one time authorized to access an organization's information system, data, or network. Such authorization implies a degree of trust in the individual. The insider threat refers to harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual.

(6) **Natural Threat**. Natural threats that can damage and disrupt cyberspace include events such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring the DOD to maintain or restore key cyberspace systems. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.

(7) **Physical Threat**. Threats are unpredictable and can take many forms. A backhoe cutting a fiber optic cable of a key cyberspace node can disrupt the operation of cyberspace. Physical threats to cyberspace and cyberspace operations should be anticipated.[26]

d. **Risk to DOD Networks and Infrastructure**. The Defense Department's own networks and systems are vulnerable to intrusions and attacks. In addition to DOD's own networks, a cyberattack on the critical infrastructure and key resources on which DOD relies for its operations could impact the U.S. military's ability to operate in a contingency. DOD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program – for many key assets, DOD has identified its physical network infrastructure on which key physical assets depend – but more must be done to secure DOD's cyber infrastructure.

e. In addition to destructive and disruptive attacks, cyber actors steal operational information and intellectual property from a range of U.S. government and commercial entities that impact the Defense Department. Victims include weapons developers as well as commercial firms that support force movements through U.S. Transportation Command (USTRANSCOM). State actors have stolen DOD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.[27]

3. **Cyber Operations against the United States (2010 – 2015)**. Although there have been hundreds, if not thousands, of cyber operations against the U.S. over the past five years, the following list includes those operations acknowledged by the U.S. Government (see Figure 2-4):

a. **2010**.

- **Insider** – Army PFC Manning was found not guilty of the most serious charge of knowingly aiding the enemy, but was convicted on 20 other specifications related to the misappropriation of hundreds of thousands of intelligence documents sent to WikiLeaks. Prosecutors alleged that Manning downloaded some 470,000 SIGACTS (from Iraq and Afghanistan) from the SIPRNET.[28]

b. **2011**.

- **Iran** – DDOS attacks on the U.S. financial sector. A group sponsored by Iran's Islamic Revolutionary Guard Corps – for conducting a coordinated campaign of distributed denial of service (DDoS) attacks against 46 major companies, primarily in the U.S. financial sector (2011-2013). These attacks, which occurred on more than 176 days, disabled victim bank websites, prevented customers from accessing their accounts online, and collectively cost the banks tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers.[29]
- **Syria** – Two Syrian hackers charged with targeting Internet sites—in the U.S. and abroad—on behalf of the Syrian Electronic Army (SEA), a group of hackers that supports the regime of Syrian President Bashar al-Assad. The affected

sites—which included computer systems in the Executive Office of the President in 2011 and a U.S. Marine Corps recruitment website in 2013. They collected usernames and passwords that gave them the ability to deface websites, redirect domains to sites controlled by the conspirators, steal e-mail, and hijack social media accounts. To obtain the login information they used a technique called "spear-phishing."[30]

c. **2012**.

- **China** – A Chinese national pleaded guilty to participating in a years-long conspiracy to hack into the computer networks of major U.S. defense contractors to steal military technical data (C-17 strategic transport aircraft and certain fighter jets) and send the stolen data to China.[31]

d. **2013**.

- **Iran** – An Iranian hacker obtained unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, NY. This allowed him to repeatedly obtain information regarding the status and operation of the dam, including information about the water levels and temperature, and the status of the sluice gate, which is responsible for controlling water levels and flow rates.[32]
- **China** – Members of PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398 charged with conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs.[33]
- **Insider**–Edward J. Snowden, was charged with violations of: Unauthorized Disclosure of National Defense Information; Unauthorized Disclosure of Classified Communication; and Theft of Government Property.[34]
- **Unattributed** – Hackers penetrated U.S. Army Corps of Engineers (USACE) database about the nation's 85,000 dams. That data included their location, condition and potential for fatalities if the dams were to be breached.[35]

e. **2014**.

- **Iran** – Computer security experts reported that members of an Iranian organization were responsible for computer operations targeting U.S. military, transportation, public utility, and other critical infrastructure networks.[36]
- **North Korea** – Conducted a cyber attack on Sony Pictures Entertainment, which stole corporate information and introduced hard drive erasing malware into the company's network infrastructure, according to the FBI.[37]
- **China** – The U.S. company, Community Health Systems, informed the Securities and Exchange Commission that it believed hackers "originating from China" had stolen personally identifiable information on 4.5 million individuals.[38]
- **Unattributed** – JP Morgan Chase suffered a hacking intrusion.[39]

- **Syria** – A member of the SEA is suspected of being responsible for a series of cyber extortion schemes targeting a variety of American and international companies.[40]
- **Unattributed** – A data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses.[41]
- **Iran** – Iranian actors have been implicated in the February 2014 cyber attack on the Las Vegas Sands casino company.[42]

f. **2015**:

- **Unattributed** – In June 2015, a Pentagon spokesman acknowledged that an element of the army.mil service provider's content was compromised. After this came to their attention, the Army took appropriate preventive measures to ensure there was no breach of Army data by taking down the website temporarily. Later, the Syrian Electronic Army (SEA) claimed responsibility for defacing the army.mil website.[43]
- **Unattributed** – the Office of Personnel Management (OPM) discovered that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective federal government employees, as well as other individuals for whom a federal background investigation was conducted.[44] OPM announced the compromise resulted in 21.5 million personal records being stolen. The Chinese government announced that it arrested a handful of hackers it says were connected to the breach of Office of Personnel Management's database.[45]
- **Russia** – Cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates.[46]
- **Insider** – A former U.S. Nuclear Regulatory Commission employee pleads guilty to attempted spear-phishing cyber-attack on Department of Energy computers to compromise, exploit and damage U.S. government computer systems that contained sensitive nuclear weapon-related information with the intent of allowing foreign nations to gain access to that information or to damage essential systems.[47]
- **Unattributed**– A "group of hackers" was responsible for an intrusion into an unclassified network maintained by the Joint Staff.[48]

Actor	2010	2011	2012	2013	2014	2015
Russia						Critical Infrastructure
China			Defense Contractors (C-17 and fighter aircraft)	Cyber Espionage	Community Health Systems	
North Korea					Sony Pictures	
Iran		DDOS against U.S. Financial Sector		Bowman Dam SCADA	Las Vegas Casino US Military Transportation	
Syria		Executive Office of the President		USMC Website	Cyber Extortion	
Insider	PFC Manning: Iraq & Afghanistan SIGACTS			Snowden: NSA leaks		Employee: DOE exploit

Figure 2-4: Cyber Operations against the United States (2010 – 2015)

4. **Cyberspace Operation Techniques**. Adversaries use a myriad of cyberspace techniques to accomplish their objectives. Some of these are:

a. **Backdoor**. This is used to describe a back way, hidden method, or other type of method of by passing normal security in order to obtain access to a secure area. It is also referred to as a trapdoor. Sometimes backdoors are surreptitiously planted on a network element. However, there are some cases where they are purposely installed to facilitate system management, maintenance, and troubleshooting operations by technicians.

(1) Security for these interfaces is normally via userids and passwords. Unfortunately, passwords are often the weakest link in a computer security scheme because password cracking tools continue to improve and the computers used to crack passwords are more powerful than ever. Network passwords that once took weeks to crack can now be cracked in hours.

(2) Although this intentional interface allows the service provider access to conduct maintenance on the equipment, many vendors build back doors to have access to these interfaces so they can also remotely troubleshoot equipment. Unfortunately, this means a technician from outside the organization is able to gain access to the system and could facilitate cyber terrorist activities.

b. **Denial of Service Attacks (DOS)**. A DOS attack is designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

c. **Distributed Denial of Service Attack (DDOS)**. An even more effective DOS is the DDOS. This involves the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the DOS from multiple paths makes backtracking the attack extremely difficult, if not impossible. Many

times worms are planted on computers to create **zombies** that allow the attacker to use these machines as unknowing participants in the attack.

d. **E-mail Spoofing (also called Phishing)**. E-mail spoofing is a method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into making a damaging statement or sent claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

e. **IP Address Spoofing**. A method that creates Transmission Control Protocol/Internet Protocol (TCP/IP) packets using somebody else's IP address. Routers use the "destination IP" address to forward packets through the Internet, but ignore the "source IP" address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

f. **Keylogger**. A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, a user can easily obtain passwords and other information the computer operator may not wish others to know.

g. **Logic bomb**. A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files. It may be brought into a computer by downloading a public-domain program that has been tampered with. Once it is executed, it does its damage immediately, whereas a virus keeps on destroying.

h. **Physical Attack**. This involves the actual physical destruction of a computer system and/or network to include transport networks as well as the terminal equipment.

i. **Sniffer**. A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere through different means.

j. **Trojan Horse**. A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

k. **Virus**. A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program.

l. **Worm**. A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.[49]

5. **Challenges**. In addition the threats mentioned above, the commander must address significant cyberspace challenges when defining the problem and producing an operational approach.

a. **Anonymity and Difficulties with Attribution**. Perhaps the most challenging aspect of attributing actions in cyberspace is connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor. This effort requires significant

analysis and collaboration with non-cyberspace agencies or organizations. The nature of cyberspace presents challenges to determining the origin of cyberspace threats.

b. **Private Industry**. Many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively. Therefore, DOD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to improve cybersecurity.[50]

V. Cyberspace Actions and the Operational Approach.

1. **Operations "*In*", "*Through*", and External to Cyberspace**. When developing an operational approach, a commander should synchronize actions '*in*' and '*through'* cyberspace with other activities to achieve the desired objectives. Actions '*in*' cyberspace are typically offensive and defensive operations that deny an adversary's use of resources or manipulate an adversary's information, information systems, or networks. On the other hand, the military operates '*through'* cyberspace on a routine basis as it conducts joint functions: command and control, intelligence, fires, movement and maneuver, protection, and sustainment. These joint functions comprise related capabilities and activities grouped together to help commanders integrate, synchronize, and direct operations (see Figure 2-5).

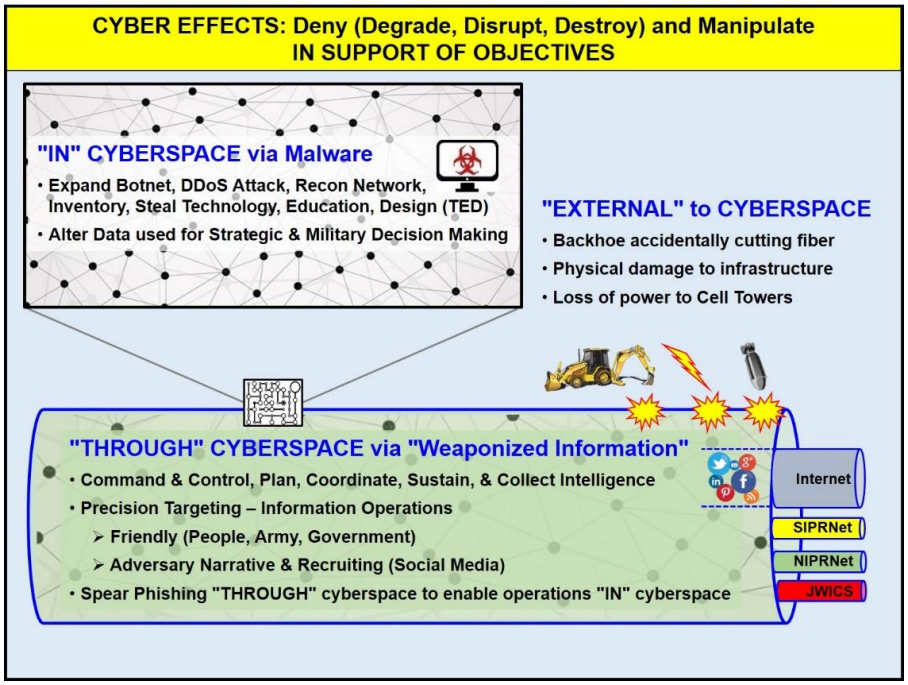

Figure 2-5: Operations Internal and External to Cyberspace

2. **U.S. Military Dependence on Cyberspace**. Commanders must be aware that U.S. military forces are critically dependent on networks and information systems to conduct operations. Nearly every conceivable component within DOD is networked. These networked systems and components are inextricably linked to the Department's ability to project military force and the associated mission assurance. Over the past decades, DOD developed its Full Spectrum Dominance doctrine that envisioned information superiority to great advantage as a force multiplier. The power of this doctrine and its near total reliance on information superiority led to networking almost every conceivable component within DOD, with frequent networking across the rest of Government, commercial and private entities, and coalition partners in complex, intertwined paths. While proving incredibly beneficial, these ubiquitous IT capabilities have also

made the U.S. increasingly dependent upon safe, secure access and the integrity of the data contained in the networks. A weakness of the implementation of this doctrine is its focus on functionality, connectivity and cost of information superiority over security—similar to the development of the Internet.

3. **Cyberspace Vulnerabilities**. The performance of U.S. military forces has demonstrated the superiority of networked systems coupled with kinetic capabilities and well-trained forces. Adversaries have discovered that the same connectivity and automation that provides great advantage to the U.S., is also a weakness that presents an opportunity to undermine U.S. capabilities in a very asymmetric way. The same network attack tools that are available on the commercial market are available to our adversaries. In addition, adversaries with financial means will invest to improve those tools and build more capable weapons to attack U.S. military systems and national infrastructure.[51]

4. **Cyberspace Operations**. Cyberspace Operations (CO) can contribute directly to the commander's visualization of the operational approach and achievement of desired effects, conditions, and end state objectives. The successful execution of (CO) requires integrated and synchronized Department of Defense information networks (DODIN), defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO) (see Figure 2-6).

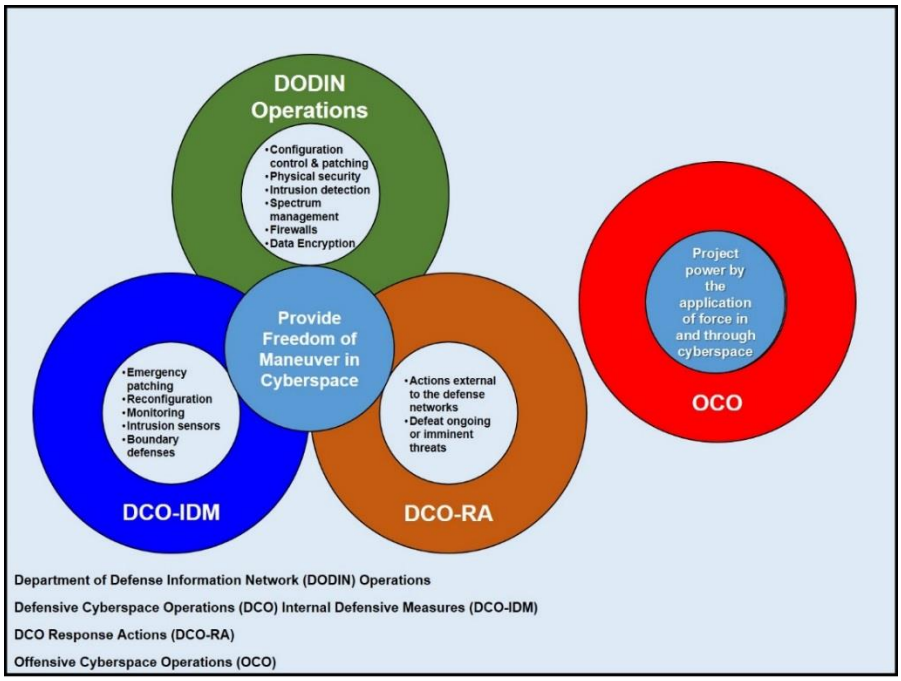

Figure 2-6: Cyberspace Operations

a. **DOD Information Network (DODIN) Operations**. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions which address the entire DODIN, including configuration control and patching, IA measures and user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data. Although many DODIN operations activities are regularly scheduled events, they should not be considered routine or unimportant, since their aggregate effect establishes the security framework on which all DOD missions ultimately depend.

b. **Defensive Cyberspace Operations (DCO)**. DCO are intended to defend DOD or other friendly cyberspace. Specifically, they are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. DCO responds to unauthorized activity or alerts/threat information against the DODIN, and leverages intelligence, counterintelligence (CI), law enforcement (LE), and other military capabilities as required. DCO includes outmaneuvering adversaries taking or about to take offensive actions against defended networks, or otherwise responding to internal and external cyberspace threats. Most DCO occurs within the defended network. Internal defensive measures include mission assurance actions to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks to ensure sufficient cyberspace access for commander forces. DCO also includes actively hunting for advanced internal threats that evade routine security measures. However, some adversary actions can trigger DCO response actions (DCO-RA) necessary to defend networks, when authorized, by creating effects outside of the DODIN. DCO consists of those actions designed to protect friendly cyberspace from adversary actions. DCO may be conducted in response to attack, exploitation, intrusion, or effects of malware on the DODIN or other assets that DOD is directed to defend. DOD's DCO mission is accomplished using a layered, adaptive, defense in- depth approach, with mutually supporting elements of digital and physical protection. A key characteristic of DOD's DCO activities is a construct of active cyberspace defense. The *Department of Defense Strategy for Operating in Cyberspace* describes active cyberspace defense as DOD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities to defend networks and systems. Leveraging the full range of DCO, active cyberspace defense builds on traditional approaches to defending DOD networks and systems to address advanced persistent threats. Defense of the DODIN and other elements of cyberspace requires situational awareness (SA) and automated, agile, and synchronized preapproved defenses. Types of DCO consist of:

(1) **DCO Internal Defensive Measures (DCO-IDM)**. Internal defensive measures are those DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, CI, LE, and other military capabilities as required.

(2) **DCO Response Actions (DCO-RA)**. DCO-RA are those deliberate, authorized defensive actions which are taken external to the DODIN to defeat ongoing or imminent threats to defend DOD cyberspace capabilities or other designated systems. DCO-RA must be authorized in accordance with (IAW) the standing rules of engagement and any applicable supplemental rules of engagement and may rise to the level of use of force. In some cases, countermeasures are all that is required, but as in the physical domains, the effects of countermeasures are limited and will typically only degrade, not defeat, an adversary's activities.

c. **Offensive Cyberspace Operations (OCO)**. OCO are intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires deconfliction IAW current policies.

d. **Cyberspace Actions**. While the commander's military missions in cyberspace (OCO, DCO, and DODIN operations) are categorized by intent, as described above, these missions will require the employment of various capabilities to create specific effects in cyberspace. To plan for, authorize, and assess these actions, it is important the commander and staff understand how they are distinguished from one another.[52]

(1) **Cyberspace information collection** is an extension of information collection consisting of actions that facilitate CO primarily through deliberate network reconnaissance and surveillance and other enabling activities (including access to or control of those networks) in and through cyberspace. Cyberspace information collection includes activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future operations and enabling activities conducted to plan and prepare for follow-on military operations. Cyberspace information collection aligns with cyberspace intelligence, surveillance, and reconnaissance and cyberspace operational preparation of the environment (see Figure 2-7).

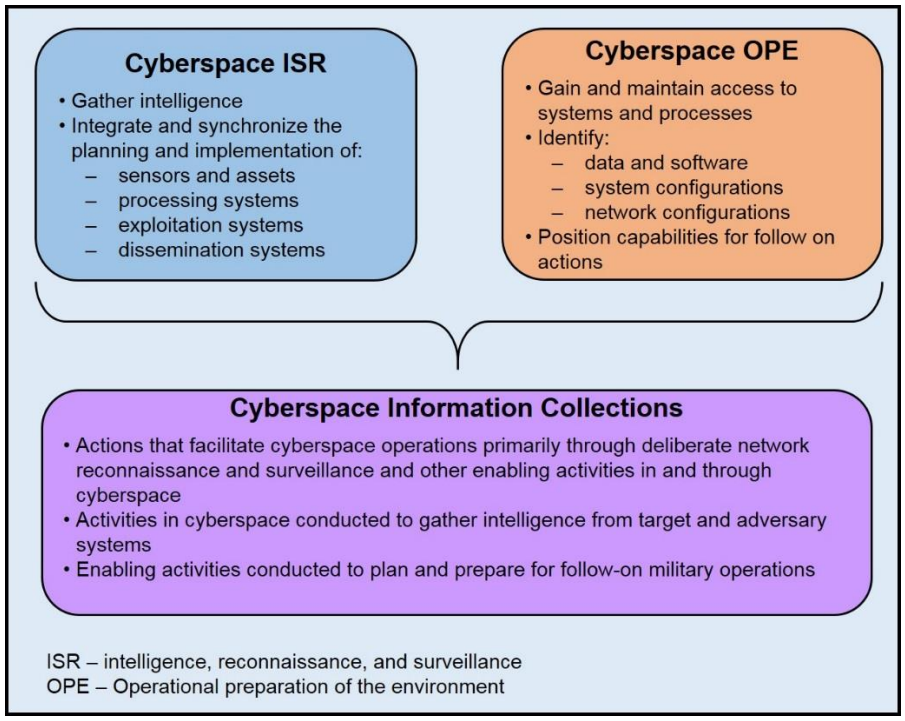

Figure 2-7: Cyberspace information collection[53]

(a) **Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)**. An intelligence action conducted by the commander authorized by an EXORD or conducted by attached signals intelligence (SIGINT) units under temporary delegated SIGINT operational tasking authority (SOTA). Cyberspace ISR includes ISR activities in cyberspace conducted to gather intelligence that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and operation of cyberspace systems, in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction, and cyberspace forces that are trained and certified to a common standard

with the intelligence community (IC). ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other U.S. government departments and agencies.

(b) **Cyberspace operational preparation of the environment** consists of the non-intelligence enabling activities conducted to plan and prepare for follow-on military operations. This includes identifying data, software, system and network configurations and identifiers, or physical structures connected to, or associated with, the network for the purposes of determining system vulnerabilities. This also includes actions taken to assure future access or control of the system, network, or data during anticipated hostilities.[54]

(2) **Cyberspace Attack**. Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. These specific actions are:

(a) **Deny**. To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.

- **Degrade**. To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified.
- **Disrupt**. To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent.
- **Destroy**. To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.

(b) **Manipulate**. To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.[55]

5. **Cross-Domain Synergy**. Cross-domain integration requires familiarity with all the domains: air, sea, land, space, and cyberspace. Cyberspace Operations enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple areas of responsibility. They can also be integrated with other information-related capabilities as part of Information Operations.

a. **Information Operations**. It is important to address the relationship between Information Operations (IO) and Cyberspace Operations. CO are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace. IO is more specifically concerned with the integrated employment of information-related capabilities during military operations, in concert with other LOOs/LOEs, to **influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own**. Thus, cyberspace is a medium through which some information-related capabilities, such as military

information support operations (MISO) or military deception (MILDEC), may be employed. However, IO also uses capabilities from the physical domains to accomplish its objectives.

b. **Electromagnetic Spectrum**. Other capabilities the commander may employ in conjunction with, or to enable CO, include significant portions of electronic warfare (EW); electromagnetic spectrum (EMS) management, command and control; ISR; navigation warfare (NAVWAR); and some space mission areas.[56]

Chapter 3: Planning

Planning translates strategic guidance and direction into campaign plans and operation orders (OPORDs). Joint operation planning may be based on defined tasks identified in strategic guidance. Alternatively, joint operation planning may be based on the need for a military response to an unforeseen current event, emergency, or time-sensitive crisis. Although the four planning functions of strategic guidance, concept development, plan development, and plan assessment are generally sequential, they often run simultaneously in the effort to accelerate the overall planning process.[57]

I. Joint Operation Planning Process (JOPP)

1. JOPP is an orderly, analytical process, which consists of a set of logical steps to examine a mission; develop, analyze, and compare alternative courses of action (COAs); select the best COA; and produce a plan or order. JOPP provides a proven process to organize the work of the commander, staff, subordinate commanders, and other partners, to develop plans that will appropriately address the problem to be solved. It focuses on defining the military mission and development and synchronization of detailed plans to accomplish that mission (see Figure 3-1).

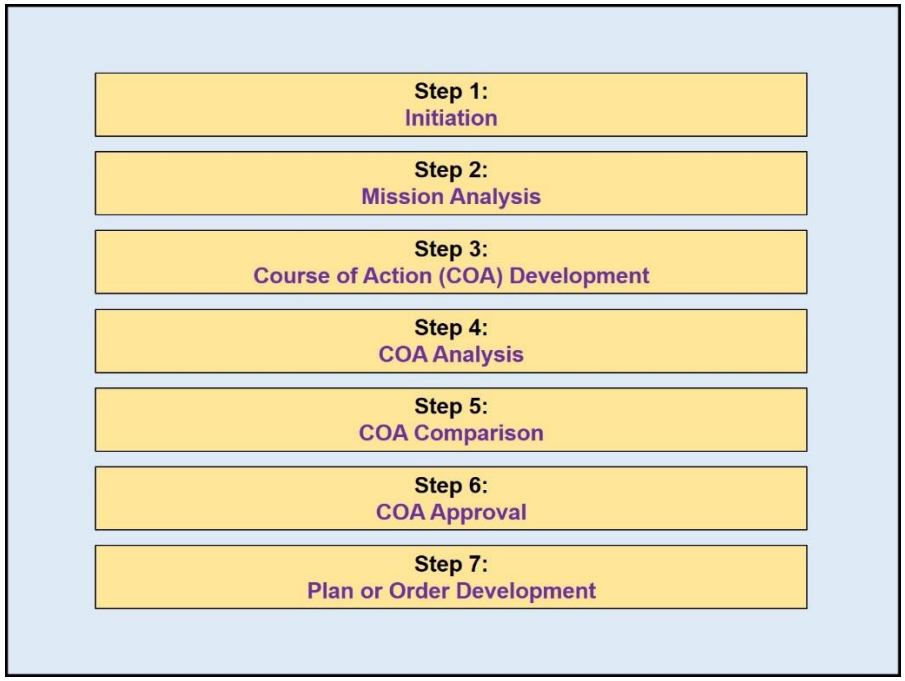

Figure 3-1: Joint Operational Planning Process[58]

a. **Initiation**. Planning begins when an appropriate authority recognizes potential for military capability to be employed in response to a potential or actual crisis. Analyses of developing or immediate crises may result in the President, Secretary of Defense (SecDef), or Chairman of the Joint Chiefs of Staff (CJCS) initiating military planning through a warning order or other planning directive. The commander typically will provide initial planning guidance based upon current understanding of the operational environment, the problem, and the initial operational approach for the campaign or operation.

b. **Mission Analysis**. Mission analysis is used to study the assigned tasks and to identify all other tasks necessary to accomplish the mission. Mission analysis is critical because it provides direction to the commander and the staff, enabling them to focus

effectively on the problem at hand. The primary products of mission analysis are staff estimates, the mission statement, a refined operational approach, the commander's intent statement, updated planning guidance, and commander's critical information requirements.

c. **Course of Action (COA) Development**. The staff develops COAs to provide unique choices to the commander, all oriented on accomplishing the military end state. Since the operational approach contains the commander's broad approach to solve the problem at hand, each COA will expand this concept with the additional details that describe who will take the action, what type of military action will occur, when the action will begin, where the action will occur, why the action is required (purpose), and how the action will occur (method of employment of forces).

d. **COA Analysis, Comparison, and Approval**. COA analysis is the process of closely examining potential COAs to reveal details that will allow the commander and staff to tentatively identify COAs that are valid, and then compare these COAs. COA analysis identifies advantages and disadvantages of each proposed friendly COA. The commander and staff analyze each tentative COA separately according to the commander's guidance. Once COA analysis is complete, the staff uses compares each COA using a subjective process whereby COAs are considered independently and evaluated/compared against a set of criteria that are established by the staff and commander. The goal is to identify and recommend the COA that has the highest probability of success against the enemy COA that is of the most concern to the commander.

e. **Plan or Order Development.** During plan or order development, the commander and staff, in collaboration with subordinate and supporting components and organizations, expand the approved COA into a detailed joint contingency plan or Operations Order (OPORD) by first developing an executable Concept of Operations (CONOPS)—the eventual centerpiece of the contingency plan or OPORD. The CONOPS clearly and concisely expresses what the commander intends to accomplish and how it will be done using available resources. It describes how the actions of the joint force components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels.[59]

II. Cyberspace Operations – Planning Considerations

1. **Planning Integration**. Cyberspace Operations (CO) encompass more than just the network connections upon which the joint force relies. **Cyberspace effects are created through the integration of cyberspace capabilities with air, land, maritime, and space capabilities**. The boundaries within which CO are executed and the priorities and restrictions on its use should be identified in coordination between the commander, non-DOD government departments and agencies, and national leadership. Effects in cyberspace may have the potential to impact intelligence, diplomatic, and law enforcement (LE) efforts and therefore will often require coordination across the interagency. CO planners are presented the same considerations and challenges that are present in planning for other joint capabilities and functions, as well as some unique considerations. Targeting, deconfliction, commander's intent, political/military assessment, and collateral effects considerations all play into the calculations of the CO planner's efforts. In a similar fashion, all of the principles of joint operations, such as maneuver and surprise, are germane to CO.

2. However, second and higher order effects in and through cyberspace can be more difficult to predict, necessitating more branches and sequels in plans. Further, while many elements of cyberspace can be mapped geographically in the physical domains, a full understanding of an

adversary's posture and capabilities in cyberspace involves understanding the underlying network infrastructure, a clear understanding of what friendly forces or capabilities might be targeted and how, and an understanding of applicable domestic, foreign, and international laws and policy. Adversaries in cyberspace may be nation states, groups, or individuals, and the parts of cyberspace they control are not necessarily either within the geographic borders associated with the actor's nationality, or proportional to the actor's geopolitical influence. A criminal element, a politically motivated group, or even an individual may have a greater presence and capability in cyberspace than many nations do today. Regardless of what operational phase may be underway, it is always important to determine what authorities are required to execute CO. Cyberspace planners must account for the lead time to acquire the authorities needed to implement the desired cyberspace capabilities. This does not change the commander's planning fundamentals, but does emphasize the importance of coordination with interagency partners, who may have authorities that are different from DOD. Despite the additional considerations and challenges of integrating CO in commander planning, planners can use many elements of the traditional processes to implement the commander's intent and guidance.[60]

3. **Cyberspace Planning and JOPP**. Cyberspace operations capability considerations and options are integrated into JOPP, just like all other joint capabilities and functions.

a. **Initiation**. During the receipt of mission, cyber planners participate in the commander's initial assessment actions and gathers the resources required for mission analysis. Unique to cyberspace, part of the initial assessment determines whether resources can be brought to bear on the mission at hand within a reasonable timeframe or context through the reachback and support processes.

b. **Mission Analysis**. Cyberspace planners contribute to mission analysis in order to help commanders understand the operational environment and frame the problem. An effective mission analysis considers the potential impact cyberspace on an operational environment. Cyberspace planners do this by participating in planning actions that help form the problem statement, mission statement, commander's intent, planning guidance, initial commander's critical information requirements, essential elements of friendly information, and updated running estimates. **Cyberspace planners coordinate with the intelligence directorate (J-2), operations directorate (J-3), communications system directorate (J-6), and other staff elements in reference to mission critical systems, risk assessments, current defense posture, and overall operational requirements**. When utilized as an information-related capability the cyberspace planners work closely with the information operations (IO) staff to identify the desired effects for the information environment.

(1) Cyberspace planners further contribute to overall mission analysis by participating in the intelligence preparation of the environment and closely coordinate with the intelligence directorate (J-2) by providing information, advice, and assistance. This ensures the intelligence staff understands what cyberspace products are needed in order for to tailor intelligence preparation of the battlefield products. Threats and vulnerabilities are identified in accordance with adversary offensive cyberspace capabilities. A friendly center of gravity analysis is conducted to ensure thorough planning. A key portion of this analysis is to assess the potential impact of cyberspace operations on friendly assets.

(2) Cyberspace planners then analyze the commander's intent and mission from a cyberspace perspective and determine if cyberspace capabilities are available to accomplish the identified tasks. If organic assets are insufficient, planners draft

cyberspace effects requests using the cyberspace effects request form (CERF). A cyberspace support element may be required to support the organic cyberspace planning team.

c. **Course of Action (COA) Development**. The cyberspace planning team contributes to COA development by determining possible friendly and enemy operations and which friendly Cyberspace capabilities are available to support the operations. Cyberspace planners focus their efforts on achieving an operational advantage at the decision point of each COA. By the conclusion of the COA development, the Cyberspace planners generate a list of cyberspace actions that will accomplish the commander's objectives and desired effects. The team also generates a list of capabilities, information, and intelligence required to perform the tasks for each COA.

d. **COA Analysis, Comparison, and Approval**. During COA analysis the cyberspace planning team coordinates with each of the warfighting function staff members to integrate and synchronize CO into each COA, thereby identifying which COA best accomplishes the mission. The cyberspace planners address how CO capabilities support each COA and apply them to timelines, critical events, and decision points. During COA comparison all staff members evaluate the advantages and disadvantages of each COA from their perspectives. The cyberspace planner present their findings for the others' consideration. At the conclusion of the COA comparison, the cyberspace planning team generates a list of pros and cons for each COA relative to cyberspace. They also develop a prioritized list of the COAs from a cyberspace perspective. The commander's final guidance provides the cyberspace planners with the commander's intent, any new critical information requirements, risk acceptance, and guidance on the priorities for the elements of combat power, orders preparation, rehearsal, and preparation.

e. **Plan or Order Development**. Cyberspace planners provide the appropriate input for several sections of the operation order or plan and associated annexes or appendixes as required. This may include input to other functional area annexes such as intelligence, fire support, signal, and civil affairs operations as required.[61]

4. **Cyberspace-Related Intelligence Requirements (IRs)**. During mission analysis, the joint force staff identifies significant gaps in what is known about the adversary and other relevant aspects of the operational environment (OE) and formulates IRs. IRs are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based on the command's IRs, the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). Information requirements related to cyberspace may include: network infrastructures, personnel status and readiness of adversaries' equipment, and unique cyberspace signature identifiers such as software/firmware versions, configuration files, etc.

5. **Information Operations (IO)**. Cyberspace Operations are one of several information-related capabilities (IRCs) available to the commander. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focus on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort.[62]

6. **Planning Insights**. Gaining insight and understanding of available cyberspace capabilities, from the experts listed above, enables planners to merge these capabilities with the other domains.

a. **Avoid symmetric thinking**. Merely because the adversary attacks through cyberspace, does not restrict us to solely cyberspace response options. Commanders and staffs should consider attaching the Cyberspace physical layer as well as conducting operations 'in' cyberspace.

b. **Identify potential cyberspace needs early** Cyberspace capabilities require long approval chains and, sometimes, long development timelines. Identify needs early in the planning process and set cyberspace planners working to secure the necessary permissions.

c. **Tailor requests for cyberspace operations**. Given cyberspace operations' global nature and potential for cascading effects, authorities rarely grant broad permissions. Planners should craft requirements which are specific (used only in certain situations, limited in duration, and limited networks affected). By requesting a discrete operation, planners increase the likelihood of approval and, potentially, shorten approval time. Planners should coordinate and socialize desired cyber activities with the IA as early as possible in planning.

d. **Conducting cyberspace damage assessment is often difficult**. A friendly cyberspace operator may report mission accomplishment. However, unlike physical munitions, there will not be a blast crater to verify results. Planners must use other ways to the measure success of a cyberspace operation. One approach is to layer assessments. For example, if a cyberspace operator reports disarming an adversary through cyberspace, probe the adversary's system with a remotely piloted vehicle before launching a risky major assault.

e. **All cyberspace operations require branch plans to accomplish similar effects.** Because offensive cyberspace operations (OCO) are often disapproved and susceptible to failure, planners must understand the intent of those cyberspace operations and develop a branch plan to accomplish that intent through other domains. Similarly, joint staff officers must understand that most of today's operating systems are vulnerable to attack. The Joint Force should prepare to operate with degraded cyberspace capabilities.

f. **Many cyberspace capabilities are classified** to avoid exposing vulnerabilities. Lack of sufficient security clearances will hinder a planner's ability to integrate cyberspace capabilities. To mitigate this challenge, lead planners should include cyberspace experts in planning team meetings to inform them of the plan's objectives and intent. This enables planners to discreetly integrate classified capabilities while informing only those with the appropriate clearance and need-to-know.[63]

III. Cyberspace Operations Planning Staff and Processes

1. **Cyberspace Planning Support**. Planners integrating cyberspace operations into a joint planning process should first seek the expertise of the cyberspace planners on their staff and those organizations provided by USCYBERCOM and its Joint Force Headquarters and Service Components (Appendix B provides an overview of U.S. cyberspace organizations). The cyberspace operations command and control (C2) architecture defines global, regional, and functional cyberspace operational lanes; enables unity of effort; and allows combatant commands (CCMDs) to use current authorities to conduct timely operations. It stresses the need for partnership among all Department of Defense (DOD) organizations conducting

operations across the three cyberspace lines of operation (LOOs) and lines of effort (LOEs) of: Department of Defense information network (DODIN) operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO) (see Figure 3-2).

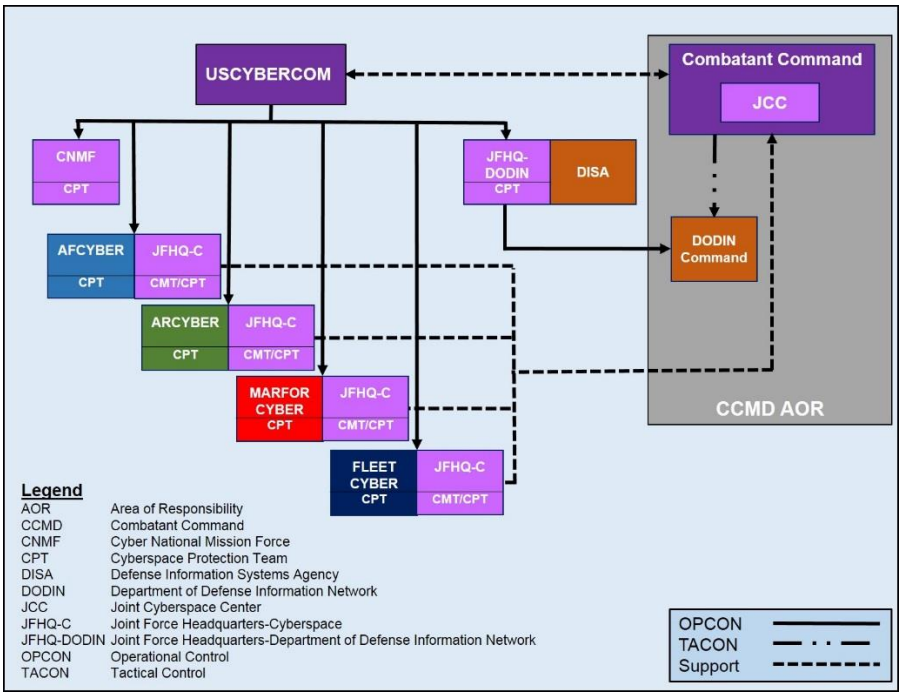

Figure 3-2: Joint Cyberspace Operations Command and Control
(adapted from JP 6-0: Figure II-1)

a. **Combatant Command (CCMD) Joint Cyberspace Centers (JCCs)**. CCDRs should size and structure the JCC to best support mission and CCMD requirements. CCMDs, through their JCC, coordinate cyberspace operations (CO) requirements and capabilities throughout their planning, operations, intelligence, targeting, and readiness processes in order to integrate and synchronize CO with all other military operations. Additionally, in partnership with USCYBERCOM, the JCC engages and coordinates regionally with interagency and multinational partners (as necessary). The JCC will:

(1) Combine inputs from USCYBERCOM with information about CCMD tactical and/or constructed networks to provide a regional/functional situational awareness (SA) / common operating picture (COP) tailored to CCMD requirements.

(2) Facilitate, through USCYBERCOM, coordination and deconfliction of CCDR directed CO which may impact or conflict with other DOD or other U.S.G cyberspace activities or operations within the area of responsibility (AOR) or DOD information networks. As early as possible in the planning process, provide USCYBERCOM with sufficient information about CCDR planned CO to enable deconfliction with U.S. government CO.[64]

b. **Joint Force Headquarters–Cyberspace (JFHQ-C)**. As a part of the Cyberspace Mission Force, USCYBERCOM designated each service's cyberspace component (AFCYBER, ARCYBER, MARFORCYBER, U.S. Fleet Cyber Command) a Joint Force Headquarters–Cyberspace and directed each one to support specific combatant commands. These headquarters provide cyberspace domain expertise, enabling the

supported combatant command staff to integrate the necessary operational- and tactical-level cyberspace planning activities into operational plans. Additionally, JFHQ-C executes OPCON to the tactical firing units known as Combat Mission Teams, which are aligned to specific target sets within their respective combatant commands. The JCC and JFHQ-C establish unity of command and unity of effort for the combatant commander's (or joint force commander's, if established) cyberspace operations through direction of the attached combat mission teams.

c. **Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DODIN)**. JFHQ-DODIN has operational control over each DODIN command for global DODIN/Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) activities supporting USCYBERCOM's global DODIN mission. The DODIN commands are tactical level headquarters supporting both global and regional combatant command (CCMD) mission needs. CCMD JCCs have tactical control of assigned DODIN commands for those DODIN and DCO-IDM activities supporting their regional CCMD missions.[65]

d. **Combat Mission Team (CMT)**. Combat mission teams concentrate on combatant commander's objectives and project power in and through cyberspace. To leverage the CMTs' capabilities, planners must request cyber effects that support the joint force commander's objectives. Just as there are a limited number of kinetic forces, so are there a limited number of combat mission teams. As a result, every request made by the joint force commander may not be immediately pursued. The JCC reviews and validates all requests by the components to ensure not only that the effect supports the respective component's objectives but also that the request is one which the combatant commander wishes to dedicate the constrained resources of the CMT towards pursuing.[66]

e. **Cyberspace Protection Team (CPT)**. CPTs conduct the Defensive Cyberspace Operations - Internal Defense Measures (DCO-IDM) mission. DCO-IDM are those actions taken internally to friendly cyberspace. In contrast, Defensive Cyberspace Operations – Response Actions (DCO-RA) are actions taken outside our information environment to stop or block an attack. CPTs hunt on friendly cyber terrain for threats that evade our security and direct appropriate internal responses. CPTs also emulate threats to test defenses. CPTs provide support to the Cyberspace National Mission Force (CNMF), USCYBERCOM's Service Components, CCMDs, and JFHQ-DODIN.[67]

2. **Cyberspace Operations Planning Team Activities**. Execution puts a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions. Cyberspace operations are integrated and synchronized into the commander's concept of operations. Fires provided by CO are employed in accordance with the targeting plan. These integrations are based on commander's guidance, desired effects, friendly capabilities, and likely enemy or adversary course of action (COA). During execution, the cyberspace planning team is responsible for monitoring the proper employment of these capabilities in accordance with the commander's guidance and ensuring the proper integration with other warfighting function capabilities based on the concept of operations.

a. Each cyberspace operations capability has diverse operational functions and requirements. These capabilities often require wide variances in times to achieve effects. The cyberspace planning team accounts for these time variances and ensures synchronization between the capabilities during execution. The effects from each

capability being utilized are then realized at the appropriate phase in the commander's scheme of maneuver.

b. During execution the cyberspace planning team performs several actions to include:

- Serving as cyberspace experts for the commander.
- Maintaining a running estimate for cyberspace operations.
- Monitoring cyberspace actions in operations and recommend adjustments during execution.
- Recommending adjustments to the commander's critical information requirements based on the situation.
- Recommending adjustments to control measures and procedures related to cyberspace operations.
- Maintaining direct liaison with the fires, signal, and intelligence cells to ensure integration and deconfliction of cyberspace operations.
- Coordinating and managing cyberspace operations taskings to subordinate units or assets.
- Coordinating requests for nonorganic cyberspace assets.
- Continuing to assist the targeting working group in target and access development and to recommend targets to attack through cyberspace operations.
- Receiving, processing, and coordinating subordinate requests for cyberspace assets during operations.
- Providing input to the overall assessment regarding the effectiveness of cyberspace operations missions.[68]

IV. Cyberspace Appendix to Operation Plans and Orders

1. **Input to Operation Plans and Orders**. Commanders and staffs will develop an appendix to Annex C (Operations) to operation plans (OPLANs) and orders (OPORDs) to describe how cyberspace operations support operations described in a base plan or order. This appendix should describe cyberspace operations support and objectives. It should include a discussion of the overall cyberspace operations concept of operations, required support, and specific details in element subparagraphs and attachments. This appendix should also contain the information needed to synchronize timing relationships of cyberspace and should include constraints, if appropriate. The following is an example of an appendix. It is a guide, and it should not limit the information contained in an actual appendix (see Figure 3-3):

APPENDIX (CYBERSPACE ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPLAN/ORDER

(U) **References:** Add any specific references to cyber electromagnetic activities, if needed.

1. (U) Situation. Include information affecting cyberspace operations (CO) that paragraph 1 of Annex C (Operations) does not cover or that needs expansion.

a. (U) Area of Interest. Include information affecting CO; cyberspace may expand the area of local interest to a worldwide interest.

b. (U) Area of Operations. Include information affecting CO; cyberspace may expand the area of operations outside the physical maneuver space.

c. (U) Enemy Forces. List known and templated locations and CO unit activities. Identify the vulnerabilities of enemy information systems and CO systems. List enemy CO operations that will impact friendly operations. State probable enemy courses of action and employment of enemy CO assets. See Annex B (Intelligence) as required.

d. (U) Friendly Forces. Outline the higher headquarters' CO plan. List plan designation, location and outline of higher, adjacent, and other CO assets that support or impact the issuing headquarters or require coordination and additional support. Identify friendly CO assets and resources that affect subordinate commander CO planning. Identify friendly forces CO vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the electromagnetic spectrum, especially if conducting joint or multinational operations. Identify and deconflict methods and priority of spectrum distribution.

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. Identify and describe other organizations in the area of operations that may impact CO or implementation of CO specific equipment and tactics. See Annex V (Interagency) as required.

f. (U) Third Party. Identify and describe other organizations, both local and external to the area of operations that have the ability to influence CO or the implementation of CO specific equipment and tactics. This category includes criminal and non-state sponsored rogue elements.

g. (U) Civil Considerations. Describe the aspects of the civil situation that impact CO. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to Annex B (Intelligence) and Annex K (Civil Affairs Operations) as required.

h. (U) Attachments and Detachments. List units attached or detached only as necessary to clarify task organization. List any CO assets that are attached or detached, and resources available from higher headquarters. See Annex A (Task Organization) as required.

i. (U) Assumptions. List any CO specific assumptions.

2. (U) **Mission**. State the commander's mission and describe CO in support of the base plan or order.

Figure 3-3: Notional Cyberspace Operations Appendix
Adapted from FM 3-38, Appendix 12 (Cyber Electromagnetic Activities)

3. (U) **Execution**.

a. Scheme of Cyber Electromagnetic Activities. Describe how CO support the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how CO tasks will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive CO measures. Identify target sets and effects, by priority. Describe the general concept for the integration of CO. List the staff sections, elements, and working groups responsible for aspects of CO. Include the CO collection methods for information developed in staff section, elements, and working groups outside the CO element and working group. Ensure subordinate units and higher headquarters receive the CO integration plan. Describe the plan for the integration of unified action and nongovernmental partners and organizations. See Annex C (Operations) as required. This section is designed to provide insight and understanding of CO and how these activities are integrated across the operational plan. It is recommended that this appendix include an understanding of technical requirements.

(1) (U) Organization for Combat. Provide direction for the proper organization for combat, including the unit designation, nomenclature, and tactical task.

(2) (U) Miscellaneous. Provide any other information necessary for planning not already mentioned.

b. (U) Scheme of Cyberspace Operations. Describe how cyberspace operations support the commander's intent and concept of operations. Describe the general concept for the implementation of planned cyberspace operations measures. Describe the process to integrate unified action partners and nongovernmental organizations into operations, including cyberspace requirements, constraints, and restraints. Identify risks associated with cyberspace operations. Include collateral damage, discovery, attribution, fratricide (to U.S. or allied or coalition networks or information), and possible conflicts. Describe actions that will prevent adversary action(s) to critically degrade the unified command's ability to effectively conduct military operations in its area of operations. Identify countermeasures and the responsible agency. List the indications and warnings, and how they will be monitored. State how the CO tasks will destroy, degrade, disrupt, and deny enemy computer networks. Identify and prioritize target sets and effect(s) in cyberspace. If appropriate, state how CO support the accomplishment of the operation. Identify plans to detect or assign attribution of adversary actions in the physical domains and cyberspace. Ensure subordinate units are conducting defensive cyberspace operations (DCO). Pass requests for offensive cyberspace operations (OCO) to higher headquarters for approval and implementation. Describe how DOD information network (DODIN) operations support the commander's intent and concept of operations. Synchronize DOD information network operations with elements reconcilable for friendly network operations (J-6). Prioritize the allocation of applications utilizing cyberspace. Ensure the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Considerations should be made for degraded network operations. (Reference appropriate annexes and appendices as needed to reduce duplication).

1) (U) Defensive Cyberspace Operations (DCO). Describe how DCO are conducted, coordinated, integrated, synchronized, and support operations to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.

(2) (U) Offensive Cyberspace Operations (OCO). Describe how OCO are coordinated, integrated, synchronized, and support operations to achieve real time awareness and direct dynamic actions and response actions. Include target identification and operational pattern information, exploit and attack functions, and maintain intelligence information. Describe the authorities required to conduct offensive cyberspace operations.

(3) (U) DOD Information Network Operations. Describe how cyberspace operations are coordinated, synchronized, and support operations integrated with the J-6 to design, build, configure, secure, operate, maintain, and sustain networks. See Annex H (Signal) as required.

Figure 3-3 (Continued): Notional Cyberspace Operations Appendix

c. (U) Tasks to Subordinate Units. List CO tasks assigned to each subordinate unit not contained in the base order.

d. (U) Coordinating Instructions. List CO instructions applicable to two or more subordinate units not covered in the base order. Identify and highlight any CO specific rules of engagement, risk reduction control measures, environmental considerations, coordination requirements between units, and commander's critical information requirements and essential elements of friendly information that pertain to CO.

4. (U) **Sustainment**. Identify priorities of sustainment for CO key tasks and specify additional instructions as required. See Annex F (Sustainment) as required.

a. (U) Logistics. Use subparagraphs to identify priorities and specific instruction for logistics pertaining to CO. See Appendix 1 (Logistics) to Annex F (Sustainment) and Annex P (Host-Nation Support) as required.

b. (U) Personnel. Use subparagraphs to identify priorities and specific instruction for human resources support pertaining to CO. See Appendix 2 (Personnel Services Support) to Annex F (Sustainment) as required.

c. (U) Health System Support. See Appendix 3 (Health System Support) to Annex F (Sustainment) as required.

5. (U) **Command and Signal**.

a. (U) Command.

(1) (U) Location of Commander. State the location of key CO leaders.

(2) (U) Liaison Requirements. State the CO liaison requirements not covered in the unit's SOPs.

b. (U) Control.

(1) (U) Command Posts. Describe the employment of CO specific command posts (CPs), including the location of each CP and its time of opening and closing.

(2) (U) Reports. List CO specific reports not covered in SOPs. See Annex R (Reports) as required.

c. (U) Signal. Address any CO specific communications requirements. See Annex H (Signal) as required.

Figure 3-3 (Continued): Notional Cyberspace Operations Appendix

V. Cyber Effects Request Form (CERF)

1. **Cyber-Enabled Effects**. An effect is a physical and/or behavioral state of a system that results from an action, a set of actions, or another effect. A desired effect can also be thought of as a condition that can support achieving an associated objective, while an undesired effect is a condition that can inhibit progress toward an objective. The commander develops plans, which can include objectives supported by measurable operational-level desired effects and assessment indicators. This may increase operational- and tactical-level understanding of the purpose reflected in the higher-level commander's mission and intent.

a. The use of effects in planning can help commanders and staff determine the tasks required to achieve objectives. The commander and planners continue to develop and refine desired effects throughout the joint operation planning process (JOPP). Monitoring progress toward creating desired effects and avoiding undesired effects continues throughout execution.[69]

b. Cyberspace operations capabilities, though they may be used in a stand-alone context, are generally most effective when integrated with other capabilities to create the commander's desired effects. Cyberspace capabilities can be used to manipulate adversary cyberspace targets through military deception (MILDEC), redirection, systems conditioning, etc., to assist with friendly mission objectives, or deny adversary functional use of cyberspace assets.

c. These effects can be created at the strategic, operational, or tactical level. Cyberspace planners should focus their efforts on conducting cyberspace actions that achieve the commander's objectives. The operational level planner is concerned with the accumulation of tactical effects into an overall operational effect. At the operational level, objectives and desired effects are developed by the commander's staff and are used to develop tasks to subordinates. Subordinate staffs use the assigned tasks to develop tactical-level objectives, tasks, subordinate targeting objectives and effects, and plan tactical actions and measures of performance (MOPs)/measures of effectiveness (MOEs) for those actions. Tactical actions typically must combine with other tactical actions to create operational level effects; however, they can have operational or strategic implications. Usually the summation of tactical actions in an operational theater will be used to conduct an operational level assessment which in turn supports the strategic level assessment (as required).[70]

d. The U.S. Army uses a Cyber Effects Request Form (CERF) to initiate planning, target development, and the delivery of fires in and through cyberspace in support of a commander's strategic end state, operational objectives, and tasks (see Figure 3-4).

Cyber Effects Request Form [CERF]

REPORT NUMBER: C090

GENERAL INSTRUCTIONS: Use to initiate planning, target development, and the delivery of fires in and through cyberspace in support of a commander's strategic endstate, operational objectives, and tactical tasks.

Reference: ATP 3-09.32.

LINE 1 – REQUESTING UNIT INFORMATION _____ (unit making report)

LINE 2 – DATE AND TIME _____ (DTG)

LINE 3 – SUPPORTED COMMAND _____ (supported major command)

LINE 4 – REQUESTING UNIT _____ (unit requesting data)

LINE 5 – POINT OF CONTACT _____ (individual initiating request)

LINE 6 – SUPPORTED OPERATION INFORMATION _____ (supported operation data)

LINE 7 – OPLAN/CONPLAN/ORDER _____ (number or name of supported OPLAN, CONPLAN, ORDER)

LINE 8 – MISSION STATEMENT _____ (commander's mission statement)

LINE 9 – COMMANDER'S INTENT _____ (specific item of commander's intent)

LINE 10 – COMMANDER'S ENDSTATE _____ (specific item of commander's endstate)

LINE 11 – CONCEPT OF OPERATION _____ (concept of operation)

LINE 12 – OBJECTIVE (STRAT/OP/TACT)

LINE 13 – OBJECTIVE/TASK _____ (tactical objective/task)

LINE 14 – COMPUTER NETWORK OPERATIONS INFORMATION ____ (network and target data)

LINE 15 – TYPE OF TARGET _____ (on call/scheduled)

LINE 16 – TARGET PRIORITY _____ (emergency/priority/routine)

LINE 17 – TARGET NAME _____ (TGT name: MIDB/EID, or O-suffix/BE number)

LINE 18 – TARGET LOCATION _____ (TGT location: IP, MAC, physical location, any or all known)

LINE 19 – TARGET DESCRIPTION _____ (facility, individual, virtual, equipment, or organization)

LINE 20 – TARGET FUNCTION _____ (target primary function)

LINE 21 – TARGET SIGNIFICANCE _____ (TGT's importance to the adversary TGT systems)

LINE 22 – CONCEPT OF CYBER OPERATION _____ (OCO: describe how cyber fires contribute to commander's objectives; DCO: assessments / detection, containment, response, investigation)

LINE 23 – TARGET EXPECTATION STATEMENT _____ (describe endstate for targeting)

LINE 24 – REMARKS _____ (amplifying information)

LINE 25 – AUTHENTICATION _____ (report authentication)

Figure 3-4: Cyber Effects Request Form (CERF)[71]

This Page Intentionally Blank

Chapter 4: Execution

I. Execution

1. **Execute Order (EXORD)**. Execution begins when the President decides to use a military option to resolve a crisis. Only the President or Secretary of Defense (SecDef) can authorize the Chairman of the Joint Chiefs of Staff (CJCS) to issue an execute order (EXORD). Depending upon time constraints, an EXORD may be the only order a commander receives. The EXORD defines the time to initiate operations and conveys guidance not provided earlier. Execution continues until the operation is terminated or the mission is accomplished.[72]

2. **Planning During Execution**. Planning continues during execution, with an initial emphasis on refining the existing plan and producing the Operation Order (OPORD) and refining the force flow utilizing employed assigned and allocated forces.

a. As the operation progresses, planning generally occurs in three distinct but overlapping timeframes: future plans, future operations, and current operations (see Figure 4-1).

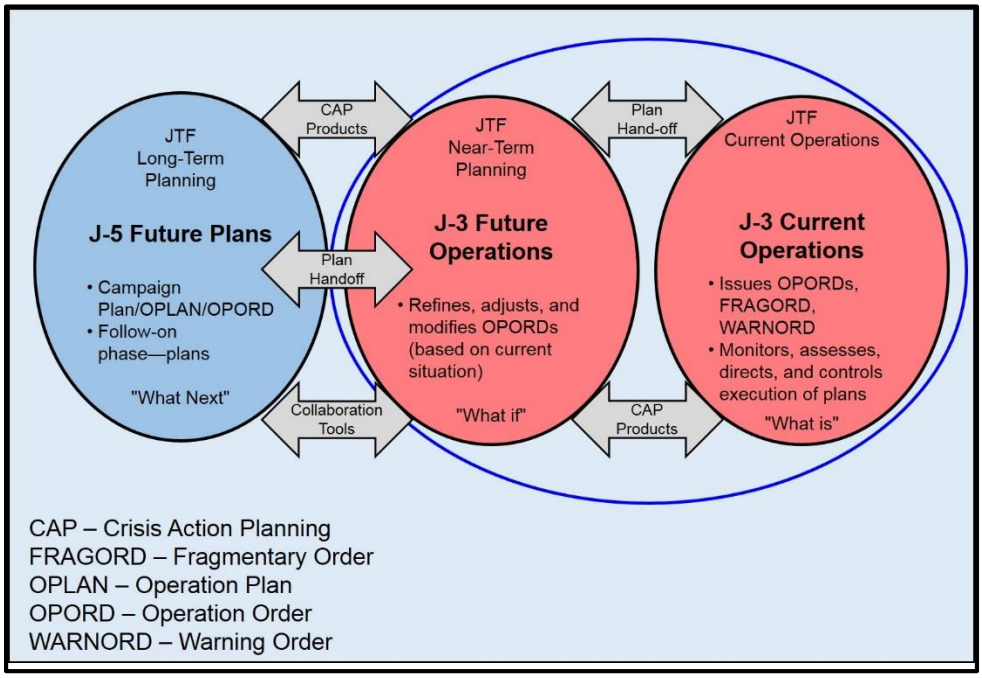

Figure 4-1: Planning During Execution[73]

(1) The plans directorate of a joint staff (J-5) focuses on future plans. The timeframe of focus for this effort varies according to the level of command, type of operation, commander desires, and other factors. Typically, the emphasis of the future plans effort is on planning the next phase of operations or sequels to the current operation. In a campaign, this could be planning the next major operation or the next phase of the campaign.

(2) Planning also occurs for branches to current operations (future operations planning). The timeframe of focus for future operations planning varies according to the factors listed for future plans, but the period typically is more near-term than the future plans timeframe. Future planning normally occurs in the J-5 or

joint planning group (JPG), while future operations planning normally occurs in the operations directorate (J-3).

(3) Finally, current operations planning addresses the immediate or very near-term planning issues associated with ongoing operations. This occurs in the joint operations center or J-3.

b. During execution, progress in meeting the commander's intent and successful accomplishment of tasks will be monitored and measured, along with the input of new data and information as it is obtained to facilitate decision making and allow for selection of branches or sequels, if applicable, or the plan to be modified as necessary.

c. Future planners must also look for opportunities or unforeseen challenges that suggest that the current mission may require revision and that a different operational approach may be required to achieve the desired end state. They should also look for indicators that the desired end state is not achievable or no longer desirable. Subsequently, these circumstances may result in a reframing of the problem and the development or execution of a branch plan or new course of action (COA).

d. Execution of a plan does not end the planning process. The planning cycle may be reentered at any point to receive new guidance, provide an in-progress review (IPR), modify the plan, decide if and when to execute branches or sequels, or terminate the operation. Planning also continues for future operations.[74]

3. **Command and Control**. How commanders organize their assigned or attached forces directly affects the responsiveness and versatility of operations. The first principle in joint force organization is that commanders organize forces to accomplish the mission based on their intent and concept of operations (CONOPS). Unity of command, centralized planning and direction, and decentralized execution are key considerations. Joint forces can be established on a geographic or functional basis. Commanders may elect to centralize selected functions within the joint force, but should avoid reducing the versatility, responsiveness, and initiative of subordinate forces. Commanders should allow Service and special operations forces (SOF) tactical and operational forces, organizations, and capabilities to function generally as they were designed. All Service components contribute their distinct capabilities to joint operations; however, their interdependence is essential to overall joint effectiveness. Joint interdependence is the purposeful reliance by one Service on another Service's capabilities to maximize the complementary and reinforcing effects of both; the degree of interdependence varies with specific circumstances. Simplicity and clarity of expression are essential.[75]

a. Mission Command is key to effective command and control. Mission Command is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander’s intent to empower agile and adaptive leaders in the conduct of unified land operations. The mission command philosophy effectively accounts for the nature of military operations. Throughout operations, unexpected opportunities and threats rapidly present themselves. Operations require responsibility and decision-making at the point of action. Through mission command, commanders initiate and integrate all military functions and actions toward a common goal—mission accomplishment.

b. The exercise of mission command is based on mutual trust, shared understanding, and purpose. Commanders understand that some decisions must be made quickly at the point of action. Therefore, they concentrate on the objectives of an operation, not how to achieve it. Commanders provide subordinates with their intent, the purpose of the operation, the key tasks, the desired end state, and resources. Subordinates then

exercise disciplined initiative to respond to unanticipated problems. Every Soldier must be prepared to assume responsibility, maintain unity of effort, take prudent action, and act resourcefully within the commander's intent.[76]

4. **Fires**. To employ fires is to use available weapons and other systems to create a specific kinetic or non-kinetic effect on a target. Joint fires are those delivered during the employment of forces from two or more components in coordinated action to produce desired results in support of a common objective. Fires typically produce destructive effects, but various non-kinetic ways and means can be employed with little or no associated physical destruction. This function encompasses the fires associated with a number of tasks, missions, and processes, including:

a. **Targeting**. This is the process of selecting and prioritizing targets and matching the appropriate response to them, taking account of command objectives, operational requirements, and capabilities.[77]

b. **Time-Sensitive Targeting**. A time-sensitive target (TST) is a target of such high priority to friendly forces that the commander designates it as requiring immediate response because it poses (or will soon pose) a danger to friendly forces, or it is a highly lucrative, fleeting target. TSTs are normally executed dynamically; however, to be successful, they require considerable deliberate planning and preparation within the joint targeting cycle.[78]

5. **Assessment**. Assessment is the continuous monitoring and evaluation of the current situation and progress of a joint operation toward mission accomplishment. It involves deliberately comparing forecasted outcomes to actual events to determine the overall effectiveness of force employment. In general, assessments should answer two questions: Is the commander doing things right? Is the commander doing the right things? More specifically, assessment helps commanders determine progress toward achieving objectives and whether the current tasks and objectives are relevant to reaching the end state. It helps identify opportunities, counter threats, and any needs for course correction, thus resulting in modifications to plans and orders. This process of continuous assessment occurs throughout the joint planning process. It is an essential tool that allows planners to monitor performance of tactical actions (measures of performance [MOPs]) and to determine whether the desired effects are created (measures of effectiveness [MOEs]) to support achievement of the objectives.[79]

a. During execution, the commander's staff identifies those key assessment indicators that suggest progress or setbacks in accomplishing tasks, creating effects, and achieving objectives. Assessment actions and measures help commanders adjust operations and resources as required, determine when to execute branches and sequels, and make other critical decisions to ensure current and future operations remain aligned with the mission and military end state.

b. Normally, the operations directorate (J-3), assisted by the intelligence directorate (J-2), is responsible for coordinating assessment activities. The chief of staff facilitates the assessment process and the determination of commander's critical information requirements (CCIRs) by incorporating them into the staff's battle rhythm. Various elements of the commander's staff use assessment results to adjust both current operations and future planning.[80]

II. Cyberspace Operations during Execution.

1. **Execution**. As the commander integrates cyberspace operations (CO) capabilities into joint operations, careful consideration must be given to some of the unique aspects of cyberspace, as well as its commonalities and synergies with operations in the physical domains: the

relationship with IO; legal, political, and technical drivers and constraints; and the role of non-DOD actors.[81]

2. **Legal Considerations**. The legal framework applicable to CO depends on the nature of the activities to be conducted, such as offensive or defensive military operations; defense support of civil authorities; service provider actions; law enforcement and counterintelligence activities; intelligence operations; and defense of the homeland. Before conducting CO, commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies, the application of which may be challenging given the ubiquitous nature of cyberspace and the often geographic orientation of domestic and international law (see Appendix A: DOD Law of War Manual excerpt).

3. **Command and Control of Cyberspace Operations**. Cyberspace Operations require coordination between theater and global operations, creating a dynamic command and control (C2) environment. CO are integrated and synchronized by the supported commander into their CONOPS, detailed plans and orders, and specific joint offensive and defensive operations. **The Geographic Combatant Commander (GCC) is generally the supported commander for CO with first order effects within their area of responsibility (AOR). Similarly, the Commander USCYBERCOM is generally the supported commander at the global or transregional (across AOR boundaries) level**. C2 of Department of Defense information network (DODIN) operations and Defensive Cyberspace Operations (DCO) may require pre-determined and preauthorized actions based on meeting particular conditions and triggers, executed either manually or automatically if the nature of the threat requires instantaneous response. The commander and planners should understand these command relationships, how they are derived and employed, and when necessary, how to deconflict them without compromising other operations. Forces conducting CO may simultaneously support multiple users. This requires extensive coordination, planning, and early integration of requirements and capabilities. Supported and supporting commanders coordinate, as appropriate, the deployment and employment of forces conducting CO required to accomplish the assigned mission. Some CO forces may be geographically separated from a particular supported theater of operations. Such cases require all involved commanders to take extra measures to ensure the supported commander is continuously aware of the remote supporting forces' operational status.

> a. Forces providing global CO capabilities may need to support multiple Combatant Commands (CCMDs) nearly simultaneously. Reachback to these capabilities allows faster adaptation to rapidly changing needs. At the same time, GCCs must be able to effectively conduct theater CO in order to operate and defend tactical and constructed networks. They must also be able to synchronize cyberspace activities related to accomplishing their operational objectives. In order to do that, some CO capabilities supporting synchronization may need to be forward deployed. However, CCMDs should retain knowledge and expertise required to support effective reachback within the CCMD, typically through the CCMD's Joint Cyberspace Center (JCC).[82]
>
> b. Mission Command. CO planning teams assist the commander in the details of planning, preparing, executing, and assessing by conducting the operations process. They use the operations process to integrate and synchronize within the headquarters and across the force. Although staffs perform many tasks, they use knowledge and information management practices to provide commanders the information they need to create and maintain their understanding and make effective decisions. Staffs also assist the commander in informing and influencing audiences. Additionally, staffs integrate and synchronize cyber electromagnetic activities across all command echelons and warfighting functions.

c. Additional commander-led and staff supported tasks reside within the mission command warfighting function. Three of these additional tasks are supported by cyberspace operations:

- Conduct military deception
- Install, operate, and maintain the network
- Conduct information protection[83]

4. **Cyberspace Synchronization**. The pace of CO requires significant pre-operational collaboration, as well as constant vigilance upon initiation, to ensure that activities in cyberspace and throughout the operational environment (OE) are coordinated and deconflicted in advance. One key to this is maintaining cyberspace SA and assessing the potential impacts to the joint force of any planned CO, including security posture, changes in configuration, or observed I&W of adversary activity. Planners and operators must also understand how operations within the OE may impact the commander's CO efforts, and vice versa. Fire support coordination measures are a method that the joint force plans and uses in the air, land, and maritime domains which facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces. Deconfliction and coordination efforts in or through cyberspace should include similar measures:

a. Deconfliction of the commander's intended offensive cyberspace operations (OCO), their activities, and the techniques planned to create these effects with other commands and agencies that may have equities in the same area of cyberspace is required. From a technical and operational perspective, deconfliction requires detailed analysis of each of the capabilities whose interoperability is being considered, as well as that of the target environment, to ensure the desired effects are achieved without unintended consequences. Additionally, the timelines required for analysis and coordination should be considered and included in the plan.

b. Planners should maintain awareness of the electromagnetic spectrum (EMS) and its impact on mobile devices and wireless networks, including cellular, wireless local area network, Global Positioning System, and other commercial and military uses of the EMS. CO and electronic attack (EA), to include offensive space control, must be deconflicted. Uncoordinated EA may significantly impact OCO utilizing the EMS. Depending upon power levels, the terrain in which they are used, and the nature of the system being targeted, unintended effects of EA can also occur outside of a local commander's AOR just as second order effects of CO may occur outside the AOR.

c. Minimizing vulnerabilities to the joint force caused by cyberspace applications. Coordinated joint force operations benefit from the use of various applications, including Web sites used for public affairs and strategic communication. Forward deployed forces also use the Internet, mobile phones, and instant messaging for logistics, morale purposes, and to communicate with friends and families. These DOD classified and unclassified networks are targeted by myriad actors, from foreign nations to malicious insiders. The commander must work with the Defense Information Systems Agency (DISA), the Services, and USCYBERCOM as well as assigned forces to limit the threat to U.S. and partner nations' networks.[84]

5. **Targeting in Cyberspace**. The purpose of targeting is to integrate and synchronize fires (the use of available weapon systems to create a specific lethal or nonlethal effect on a target) into joint operations. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. However, three aspects of CO should be included in the commander's targeting processes: recognizing

that cyberspace capabilities are a viable option for engaging designated joint targets; understanding that a CO option may be preferable in some cases; and first, second, and third order effects on joint targets may involve or affect elements of the DODIN. Additionally, there are some characteristics unique to cyberspace targets and cyberspace capabilities that are described below.

a. **Targets in Cyberspace**. Every target has distinct intrinsic or acquired characteristics. These characteristics form the basis for target detection, location, identification, target value within the adversary target system, and classification for future surveillance, analysis, strike, and assessment. As discussed earlier, cyberspace can be viewed as consisting of three layers: physical network, logical network, and cyber-persona. The challenge in targeting is to identify, coordinate, and deconflict multiple activities occurring across multiple layers.

(1) The **physical network** layer is the medium where the data travels. It includes wired (land and submarine cable) and wireless (radio, radio-relay, cellular, satellite) transmission means. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute useful targeting data in cyberspace.

(2) The **logical network** layer constitutes an abstraction of the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical dimension of the information environment is lost.

(3) The **cyber-persona** layer, an individual's or groups' online identity(ies), holds important implications for joint forces in terms of positive target identification and affiliation, and activity attribution. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and SA of a cyber-persona to enable effective targeting and creation of the commander's desired effects.[85]

b. **Target Development in Cyberspace**. Target development should be requested much earlier than that for traditional targets and should have a longer-term focus. More often, full target development takes weeks, months, or years instead of days.[86] This is due to the additional lead time necessary to generate intelligence for the offensive cyberspace effects. During deliberate planning, the capabilities analysis phase seeks to match apportioned assets and ordnance with the target and effect desired. Once a target is selected to be serviced by traditional means, it is periodically reviewed during the plan review cycle. No further resources are expended on maintaining access to the target until the plan is executed. By contrast, designating a target to be engaged with OCO starts the immediate allocation and expenditure of additional resources. Maintaining and developing a target requires a significant amount of time
(see Figure 4-2).[87]

(1) **Mission**. Due to the technical and sensitive nature of cyberspace operations, the commander will normally approve planning based on an initial concept of operations. Planners should consider cyber-enabled effects to accomplish the commander's objectives. Cyberspace capabilities must operate and create effects within the complex and ever-changing systems in cyberspace; however, they are each developed with certain environmental assumptions and

expectations about the operating conditions that will be found in the target environment.[88]

(2) **Intelligence, Surveillance, and Reconnaissance**. After receiving the commander's approval, the cyberspace operations team attempts to gain access and understand the targeted system.

- **Access**. The first step to engage a target with OCO is to gain access to it. Without physical or electronic access to the target, it is impossible to proceed with OCO. A system linked to the Internet is, in general, more accessible, though getting into its targeted portions may be challenging due to its own network security environment. A closed system would require insider access to gain firsthand knowledge of the computing environment in the target facility. Once forces gain access to a target system, they need to maintain it as long as they might wish to strike the target. Network upgrades or system changes made in the regular maintenance of the target could make it difficult to maintain or regain access. The risk from gaining access to a system is that an adversary might detect the hacking well before the attack. The adversary would discover which systems were being targeted. Moreover, discovery would assuredly result in access being lost – and the possibility of the adversary studying the attack to understand U.S. cyberspace operations and develop better defenses or even counterattacks.
- **Understanding**. Once access is gained, the next step is to learn the unique internal attributes of the targeted system. Cyberspace operations teams may need to acquire the software being targeted so they can determine its nature and vulnerabilities. Depending on the system to be attacked, the code might be commented in a language other than English. If cyberspace teams are unable to gain technical insight into the targeted software, then OCO cannot proceed; coordinating the proper effect is impossible. The commander must consider these attributes of OCO when setting target priorities during deliberate planning.

(3) **Capability Development**. Once the cyberspace operations team has developed a means for continuous access and learned the targeted system, they must then coordinate acquisition or development of the weapon with which to attack it. Some weapons designed to attack common operating systems such as Windows are commercially available. However, systems produced and used only in certain countries typically require forces to develop weapons from scratch. Developing a cyber weapon is a complex challenge. Once a weapon has been developed, the cyberspace operations teams must constantly maintain access to and monitor the target. They must ensure routine system maintenance does not nullify their labors. All of these actions require a significant amount of time, perhaps months, before anything besides a rudimentary attack can be launched with a presumption of success. Furthermore, depending on the target and its accessibility, a weapon may need to navigate through several networks to its intended target.

(4) **Execution**. After the cyberspace operations teams gain access and develop a capability, the proposed operation is reviewed for collateral damage issues and

legal concerns. USCYBERCOM, in coordination with the applicable Service Component/Joint Force Headquarters – Cyber (JFHQ-C), determines if resources are available to service the commander's target request.[89] If all these criteria are met, the commander directs an Execution Order (EXORD) for the specific cyberspace operation.

- **Cascading and Collateral Effects**. Overlaps between military, civil, government, private, and corporate activities on shared networks in cyberspace make the evaluation of probable cascading and collateral effects particularly important when planning for CO. Due to policy concerns, an EXORD or applicable rules of engagement (ROE) may limit CO to only those operations that result in no or low levels of collateral effects. A collateral effects analysis to meet policy limits is separate and apart from the proportionality analysis required by the law of war. Even if a proposed CO is permissible after a collateral effects analysis, the proposed operation must also be permissible under a law of war proportionality analysis.
- **Target Nomination and Synchronization**. Component commanders, national agencies, supporting commands and/or the staff submit target development nominations to the targeting staff for development and inclusion on the joint target list (JTL). Once identified on the JTL, targets can be selected for engagement by organic assets (if within a component commander's assigned area of operations) or nominated for action by other joint force components and other organizations, usually via a coordinating body (joint fires element [JFE] of the operations directorate of joint staff) or working group (joint targeting working group [JTWG]). The JFE normally holds a JTWG for prioritization of the nominated targets through a draft joint integrated prioritized target list (JIPTL) and establishment of the "cut line." The "cut line" simply reflects an estimate of resources available to take action against targets in priority order and does not guarantee that a specific target will be attacked. The joint targeting coordination board (JTCB) provides a senior level forum in which all components can articulate strategies and priorities for future operations to ensure that they are synchronized and integrated. Although most targeting issues are worked out at the JTWG, the JTCB normally conducts final coordination of the JIPTL and submits it for commander approval. The JFE also maintains the restricted target list and no-strike list. The no-strike list contains objects or entities that are not legal targets, while, the restricted target list is constrained by the commander for other reasons characterized as protected from the effects of military operations under international law and/or the rules of engagement.[90]

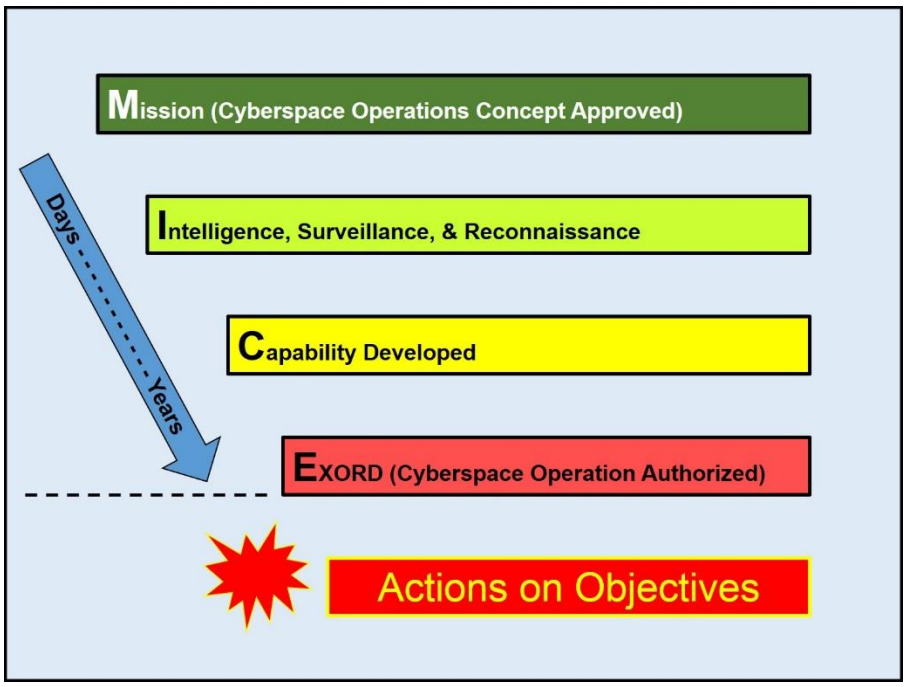

Figure 4-2: Cyberspace Target Development

c. **Time-Sensitive Targeting**. Time-sensitive targets (TSTs) that are engaged through CO require detailed joint, cross-CCMD, interagency, and likely multinational planning and coordination of OPE, engagement, assessment, and intelligence efforts. The actual prosecution of a TST through cyberspace requires that cyberspace planners and operators coordinate with the supported commander early in the planning phase to ensure access to the target is available when the fleeting opportunity arises. In addition, commanders should establish procedures to quickly promulgate execution orders for CO-engaged TSTs, which due to their unique cyberspace interagency deconfliction/coordination requirements may involve coordinating pre-approval for specific actions conducted under specific circumstances. Likewise, successful prosecution of TSTs requires a well-organized and well-rehearsed process for sharing sensor data and targeting information, identifying suitable strike assets, obtaining mission approval, and rapidly deconflicting weapon employment. The key for success is performing as much coordination and decision making as possible in advance.[91]

d. **Multinational Considerations**. Allies and coalition partners often require approval of the CO portion of plans and orders from higher authority, which may significantly impede CO implementation. Additionally, this national-level approval requirement increases potential constraints and restraints upon the participating national forces, and further lengthens the time required to gain national approval for their participation. Commanders and planners should be particularly sensitive to national agendas and anticipate the additional time required for approval through this parallel national command structure.[92]

6. **Authorities**. Authority for actions undertaken by the Armed Forces of the United States is derived from the U.S. Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace. Key statutory authorities that apply to DOD include Title 10, United States Code (USC), *Armed Forces*; Title 50, USC, *War and National Defense*; and Title 32, USC, *National Guard*. See Figure 4-3 for a summary of applicable titles of USC as they apply to cyberspace operations.[93]

United States Code (USC)	Title	Key Focus	Principle Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Security Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18	*Crimes and Criminal Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and civil support training and operations, in the US	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC, Armed Forces)
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure US interests by conducting military and foreign intelligence operations in cyberspace

Figure 4-3: United States Code-Based Authorities[94]

7. **Cyberspace Assessment**. Cyberspace Operations should be considered in the development of operational level MOPs/MOEs. In some cases, activities in cyberspace alone will have operational level effects; for example, the use of a cyberspace attack to bring down or corrupt the adversary headquarters network could very well reverberate through the entire Joint Operations Area (JOA). A CO option may be preferable in some cases.

a. Assessments in cyberspace may be unique in that the normal assessment cell will not typically have the capabilities or expertise to assess CO; CO will typically involve multiple commands, such as the supported Joint Force Commander (JFC), CDRUSCYBERCOM, and possibly other functional supporting JFCs.

b. Additionally, with CO typically being conducted as part of a larger operation, assessment of CO will need to be conducted in the context of supporting the overarching commander's objectives. Therefore, CO assessments will require close coordination within each staff and across multiple commands. Coordination and federation of the assessment efforts will often require arrangements that need to be in place prior to execution.[95]

8. **Operational Challenges**. CO may not require physical proximity; many CO can be executed remotely. Moreover, the effects of CO may extend beyond a target, a joint operations area (JOA), or even an AOR. Because of transregional considerations or the requirement for high-demand, low-density resources, CO may be coordinated, integrated, and synchronized with centralized execution from a location outside the AOR of the supported commander. Another challenge facing the commander is that the use of a capability may reveal its functionality and compromise future effectiveness. This has implications for OCO, but it also affects DCO as the same capabilities may have a role in both OCO and DCO.[96]

Chapter 5: Operations in the Homeland

"Much of our critical infrastructure – our financial systems, our power grid, health systems – run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. Foreign governments and criminals are probing these systems every single day."

President Barrack Obama[97]

I. Department of Defense Missions in the Homeland

1. The mission of the Department of Defense (DOD) is to provide the military forces needed to deter war and to protect the security of the U.S. The U.S. employs all instruments of national power to continuously defeat threats to the homeland. DOD executes the homeland defense (HD) mission by detecting, deterring, preventing, and defeating threats from actors of concern as far forward from the homeland as possible.

2. The U.S. homeland is the physical region that includes the continental United States (CONUS), Alaska, Hawaii, U.S. territories, and surrounding territorial waters and airspace. The homeland is a functioning theater of operations, and the DOD regularly performs a wide range of defense operations within the theater. **Homeland Defense is the protection of U.S. sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats as directed by the President.** An external threat or aggression is an action, incident, or circumstance that originates from outside the boundaries of the homeland. Threats planned, prompted, promote d, caused, or executed by external actors may develop or take place inside the boundaries of the homeland. The reference to external threats does not limit where or how attacks may be planned and executed. DOD is responsible for the HD mission, and leads the response with support from international partners and United States Government (USG) departments and agencies. HD is executed across the active, layered defense construct composed of the forward regions, the approaches, and the homeland.

3. By law, DOD is responsible for two missions in the homeland: HD and defense support of civil authorities (DSCA). Two geographic combatant commanders (GCCs) are the supported commanders for HD in their AORs, with virtually all other combatant commanders (CCDRs) supporting them. Commander, United States Northern Command (CDRUSNORTHCOM) and Commander, United States Pacific Command (CDRUSPACOM) are charged with specific responsibilities for HD and DSCA. HD, DSCA, and homeland security (HS) operations or events may occur simultaneously.

4. Operations in the homeland environment (both HD and HS) require pre-event and ongoing coordination with interagency, intergovernmental (i.e. federal, state, local, and tribal), and multinational partners to integrate capabilities and facilitate unified action. In this complex environment there are numerous threats across multiple jurisdictions that are addressed by a diverse group of actively involved stakeholders to include intergovernmental organizations (IGOs), multinational partnerships, nongovernmental organizations (NGOs), and the private sector. DOD plans and prepares to operate in concert with other USG entities (see Figure 5-1).

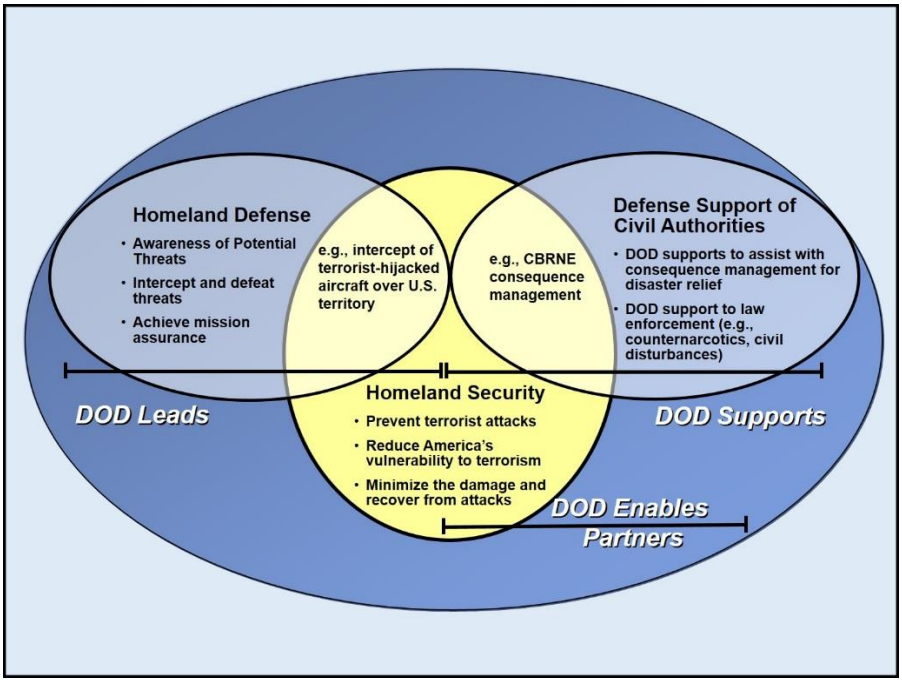

Figure 5-1: Active, Layered Defense of the United States

a. **Homeland Security (HS)**. The Department of Homeland Security (DHS) is the lead federal agency (LFA) for HS. HS is a concerted national effort to prevent terrorist attacks within the U.S.; reduce domestic vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. HS is typically conducted by federal, state, tribal, and/or local government organizations in conjunction with the private sector; and includes law enforcement (LE) activities related to countering terrorism and other criminal activities. For HS, DOD may conduct DSCA in response to requests for assistance from civil authorities, supporting a lead interagency partner such as DHS or Department of Justice (DOJ), or in some cases, a state governor. DOD support must be formally requested by the applicable civil authority and then approved by the President or Secretary of Defense (SecDef).

b. **Homeland Defense (HD)**. HD is a DOD mission. DOD is the USG lead agency responsible for defending against traditional external threats or aggression (e.g., nation-state conventional force or weapons of mass destruction [WMD]) attack and against external asymmetric threats. During HD operations, DOD coordinates with other interagency partners that may be undertaking simultaneous operations to counter the same or other threats.

c. **Defense Support of Civil Authorities (DSCA)**. DSCA is support provided by U.S. federal military forces, DOD civilians, DOD contract personnel, DOD component assets, and National Guard (NG) forces (as applicable under Title 10, USC, Section 12304 or Title 32, USC, Section 502) in response to requests for assistance from civil authorities for domestic emergencies, LE support, and other domestic activities, or from qualifying entities for special events. HD and DSCA missions may occur simultaneously and require extensive coordination, integration, and synchronization.

d. **Emergency Preparedness (EP)**. DOD may also be required to engage in emergency preparedness. EP are measures taken in advance of an emergency to reduce the loss of

life and property and to protect a nations institutions from all types of hazards through a comprehensive emergency management program of preparedness, mitigation, response, and recovery. EP is considered a part of DOD's overall preparedness activities. It is not a stand-alone activity, but is an integral part of DOD training, mitigation, and response for both HD and DSCA.[98]

II. Critical Infrastructure

1. The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family.

2. Overall, there are 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The following is a list of each critical infrastructure sector and the responsible governmental organization:

- **Chemical Sector** – Department of Homeland Security
- **Commercial Facilities Sector** – Department of Homeland Security
- **Communications Sector** – Department of Homeland Security
- **Critical Manufacturing Sector** – Department of Homeland Security
- **Dams Sector** – Department of Homeland Security
- **Defense Industrial Base Sector** – Department of Defense
- **Emergency Services Sector** – Department of Homeland Security
- **Energy Sector** – Department of Energy
- **Financial Services Sector** – Department of the Treasury
- **Food and Agriculture Sector** – Department of Agriculture and Department of Health and Human Services
- **Government Facilities Sector** – Department of Homeland Security and General Services Administration
- **Healthcare and Public Health Sector** – Department of Health and Human Services
- **Information Technology Sector** – Department of Homeland Security
- **Nuclear Reactors, Materials, and Waste Sector** – Department of Homeland Security
- **Transportation Systems Sector** – Department of Homeland Security and Department of Transportation
- **Water and Wastewater Systems Sector** – Environmental Protection Agency[99]

III. Defense Critical Infrastructure Program

1. **Homeland Security Presidential Directive-7 (HSPD-7)**, Critical Infrastructure Identification, Prioritization and Protection, assigns responsibilities to the Department of Defense. The DOD has two roles for critical infrastructure protection, first as a Federal department and second as a Sector-Specific Agency for one of 16 national infrastructure sectors-the Defense Industrial Base.

2. **Director of Mission Assurance**. Within DOD, the Assistant Secretary of Defense for Homeland Defense and Global Security, ASD(HD&GS), is assigned as the lead official for providing policy, guidance, oversight, and resource advocacy for these roles. The Director of Critical Infrastructure Protection under the ASD(HD&GS) oversees the day-to-day execution of HSPD-7 responsibilities. The responsibilities for each of these roles are summarized below:

a. **Federal Department**. As a Federal department, DOD has both departmental and national responsibilities. Departmental responsibilities include the identification, prioritization, assessment, remediation, and protection of defense critical infrastructure. Additionally, all Federal departments and agencies work together at a national level to "prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit" critical infrastructure and key resources. DOD and the broader Federal government will work with State and local governments and the private sector to accomplish this objective.

b. **Sector-Specific Agency**. As the Sector-Specific Agency for the Defense Industrial Base, DOD has the responsibilities to:

(1) Collaborate with all relevant federal departments and agencies, state and local governments, and the private sector, including key persons and entities in their infrastructure sector;

(2) Conduct or facilitate vulnerability assessments of the sector;

(3) Encourage risk-management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources; and

(4) Support sector-coordinating mechanisms:

- to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and
- to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.[100]

IV. Cyberspace Operations in the Conduct of Homeland Defense

1. **DOD Cyber Strategy**. The U.S. conducts operations, including HD, in a complex, interconnected, and increasingly global operational environment to include the cyberspace domain. The DOD Cyber Strategy sets five strategic goals for its cyberspace missions. One of these goals it to **be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence**. The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat a cyberattack of significant consequence on the U.S. homeland and U.S. interests. The Defense Department must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks before they can impact U.S. interests. Consistent with all applicable laws and policies, DOD requires granular, detailed, predictive, and actionable intelligence about global networks and systems, adversary capabilities, and malware brokers and markets. To defend the nation, DOD must build partnerships with other agencies of the government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace. The Defense Department is focused on building the capabilities, processes, and plans necessary to succeed in this mission (See Figure 5-2).[101]

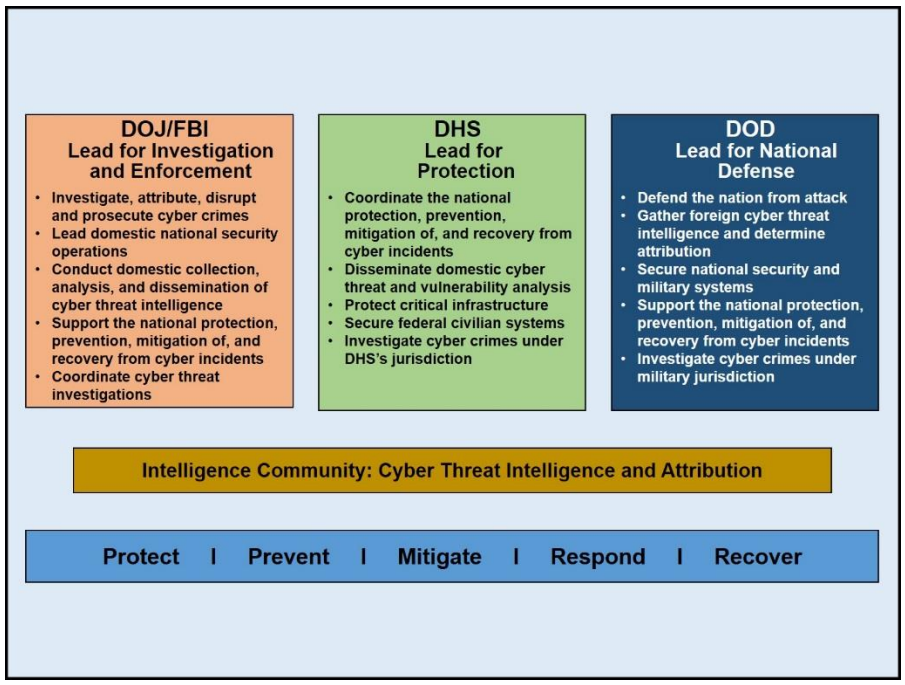

Figure 5-2: National Cybersecurity Roles and Responsibilities

2. **Unified Action**. For cyberspace, the open vulnerability and complex interrelationship of national and international networks demands closely coordinated action among the military and other government entities at all levels. The CCMDs joint cyberspace centers (JCCs), the Services, and the United States Cyber Command (USCYBERCOM), are the military front line of defense. The Secretary of Homeland Security has statutory primary agency responsibilities as the focal point for the security of cyberspace, and established the National Cyber Security Division (NCSD) within DHS for protecting USG, state and local governments, and public networks against cyberspace intrusions and attacks. USPACOM and USNORTHCOM, because of their HD and HS responsibilities, have coordination requirements for cyberspace operations through their JCCs with USCYBERCOM and potentially with NCSD, if that is not done through USCYBERCOM.[102]

a. USCYBERCOM synchronizes planning for cyberspace operations, to include direction of DOD information network (DODIN) operations and defense to secure, operate, and defend DOD networks, and to defend U.S. critical cyberspace assets, systems, and functions. Directs DODIN operations and defense in coordination with CJCS and CCMDs. Coordinate with other CCMDs and appropriate USG departments and agencies prior to the generation of cyberspace effects that cross AORs in response to cyberspace threats.

b. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities for offensive and defensive cyberspace operations and defense of DODIN; and when directed, conducts cyberspace operations to enable actions in the physical domains, facilitates freedom of action in cyberspace, and denies the same to adversaries. USCYBERCOM can support HD cyberspace operations in collaboration with USNORTHCOM, USPACOM, and DHS, by coordinating activities within the required AOR and assisting with expertise and capabilities directed and made available.[103]

3. **Command and Control (C2) of Cyberspace Operations**.

a. **CDRUSNORTHCOM** is responsible to defend against, mitigate, and defeat cyberspace threats against specific USNORTHCOM and NORAD systems, in coordination with USCYBERCOM and USPACOM. Geographic and functional CCDRs, as well as the Services, are responsible for protecting their networks located within the USNORTHCOM AOR which are not specifically assigned or attached to USNORTHCOM.[104]

b. **CDRUSPACOM** is responsible for protection of USPACOM networks in the USPACOM AOR. USPACOM will coordinate cyberspace operations with its component commands, subordinate unified commands, JTFs, direct reporting units, and other CCMDs through the USPACOM JCC. CDRUSCYBERCOM, is the supporting commander for cyberspace operations within the USPACOM AOR. USCYBERCOM normally provides a cyberspace operations teams to USPACOM for major exercises and operations. For HD, USPACOM and USCYBERCOM have coordination requirements with DHS through its NCSD as primary agency for protecting USG and public networks against cyberspace intrusions and attacks. Functional CCDRs and the Services are responsible for protection of their networks located within the USPACOM AOR, but not assigned or attached to USPACOM.[105]

4. **Cyberspace Operations Teams and Missions**. Defending the nation in cyberspace requires a military capability, operating according to traditional military principles of organization for sustained expertise and accountability at a scale that lets us perform multiple missions simultaneously.

a. The application of military capability at scale is what the Cyber Mission Force (CMF) gives USCYBERCOM and in DOD as a whole. Combat Mission Teams (CMTs) operate with the combatant commands to support their missions, while National Mission Teams (NMTs) help defend the nation's critical infrastructure from malicious cyber activity of significant consequence. Cyber Protection Teams (CPTs) defend DOD Information Networks alongside local Computer Network Defense Service Providers (CNDSPs). Each of them complements the efforts of the others. Cyber Mission Force teams can and do contribute to the nation's cyberspace efforts as they assist the combatant commands and partner departments and agencies.

b. Cyber Mission Force teams give USCYBERCOM the capacity to operate on a full-time, global basis on behalf of the combatant commands. The Combat Mission Teams help combatant commanders accomplish their respective missions to guard U.S. interests and project the nation's power when authorized to deter those who would threaten our security—the teams help ensure that we have the ability to enable our combatant commanders to defeat emerging threats. Additional Combat Mission Teams under the functional commands (U.S. Strategic Command, U.S. Transportation Command, and U.S. Special Operations Command) bring still more resources to supplement those of the regional commands.

c. USCYBERCOM controls additional teams under the Cyber National Mission Force (CNMF) that help defend the nation's critical infrastructure against malicious cyber activity of significant consequence. The CNMF comprise National Mission Teams, National Support Teams, and National Cyber Protection Teams to conduct full-spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber actors.

d. USCYBERCOM established the Joint Force Headquarters (JFHQ-DODIN) and dual-hatted the Director of the Defense Information Systems Agency (DISA) to command it.

As a functional component command of USCYBERCOM located at DISA, JFHQ-DODIN leads the day-to-day defense of DOD's data and networks. DOD is working to harden and defend its networks and systems, with USCYBERCOM providing the operational vision and directing the defense, and the DOD Chief Information Officer (CIO), working with NSA, DISA and the military services, providing the technical standards and implementation policy. DOD CIO measures the cyber security status of the whole department. The goal is to minimize the adversary's ability to attack our systems and networks, and to detect, diagnose, contain, and eject an adversary should an attack occur.

e. Operations to defend DOD networks and the nation's critical infrastructure are conducted in conjunction with a host of federal, industry, and international partners. Defending the U.S. in cyberspace is a whole-of-government, indeed a whole-of-nation, endeavor. No single agency or department has the authority, information, or wisdom to accomplish this mission alone, which is why USCYBERCOM and NSA recently updated their memorandums of understanding with DHS in a cyber action plan to chart collaboration. The entire federal government, however, cannot do the job without the active participation and cooperation of the private sector.[106]

5. **Critical Infrastructure/Key Resources (CI/KR) Protection**. The increased use of cyberattacks as a political instrument reflects a dangerous trend in international relations. Vulnerable data systems present state and non-state actors with an enticing opportunity to strike the United States and its interests. During a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage. A sophisticated actor could target an industrial control system (ICS) on a public utility to affect public safety, or enter a network to manipulate health records to affect an individual's well-being. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.[107] CI/KR consist of the infrastructure and assets vital to the nation's security, governance, public health and safety, economy, and public confidence. Concurrent with its national defense and incident response missions, DOD will also support DHS and other USG departments and agencies to ensure all sectors of cyberspace CI/KR are available to support national objectives. CI/KR protection relies on analysis, warning, information sharing, vulnerability identification and reduction, mitigation, and aiding of national recovery efforts.

a. **Defense Critical Infrastructure (DCI)**. DCI refers to DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide that are a subset of CI&KR. GCCs have the responsibility to prevent the loss or degradation of the DCI within their AORs and must coordinate with the DOD asset owner, heads of DOD components, and defense infrastructure sector lead agents to fulfill this responsibility. The Director of DISA is responsible for matters pertaining to the identification, prioritization, and remediation of critical DODIN infrastructure issues, as the lead agent for the DODIN sector of the DCI. Likewise, DOD is responsible to support the DHS coordination of efforts to protect the DIB and the DODIN portion of the DIB.[108]

b. **DOD Reliance on Critical Infrastructure**. The Defense Department must further develop adequate warning intelligence of adversary intentions and capabilities for conducting destructive and disruptive cyberattacks against DOD and the United States. Beyond its own networks, DOD relies on civil critical infrastructure across the United States and overseas for its operations, yet the cybersecurity of such critical infrastructure is uncertain. A cyberattack on the critical infrastructure and key resources on which DOD

relies for its operations could impact the U.S. military's ability to operate in a contingency.

c. **Critical Infrastructure Owners' Responsibilities**. The Defense Department cannot, however, foster resilience in organizations that fall outside of its authority. In order for resilience to succeed as a factor in effective deterrence, other agencies of the government must work with critical infrastructure owners and operators and the private sector more broadly to develop resilient and redundant systems that can withstand a potential attack. Effective resilience measures can help convince potential adversaries of the futility of commencing cyberattacks on U.S. networks and systems. [109]

d. **DOD Exercise Program**. DOD's annual exercise program, to include Cyber Guard, includes exercising with DHS and the Federal Bureau of Investigation (FBI) for contingencies that may require emergency allocation of forces to help protect critical infrastructure, under partner agencies' lead. This framework describes how combatant commands and combat support agencies can partner with DHS and FBI and other agencies to improve integration, training and support.

e. **National Guard**. DOD works with the National Guard to define the coordinate, train, advise, and assist (C/TAA) roles of the National Guard force and refine implementation through Cyber Guard exercises. Under its existing and planned force structure, National Guard forces will exercise to coordinate, train, advise, and assist state and local agencies and domestic critical infrastructure and to provide support to law enforcement, HD, and DSCA activities in support of national objectives.[110]

6. **Defense Industrial Base (DIB)**. In accordance with the National Infrastructure Protection Plan, DOD is designated as the sector-specific agency for the DIB. DOD provides cyberspace analysis and forensics support via the DIB Cybersecurity and Information Assurance Program and the DOD Cyber Crime Center.[111] The Defense Department will improve accountability and responsibility for the protection of data across DOD and the DIB. DOD will ensure that policies and any associated federal rules or contract language requirements have been implemented to require DIB companies to report data theft and loss to the Defense Cyber Crime Center.

a. DOD will continue to assess Defense Federal Acquisition Regulation Supplement (DFARS) rules and associated guidance to ensure they mature over time in a manner consistent with known standards for protecting data from cyber adversaries, to include standards promulgated by the National Institute of Standards and Technology (NIST).

b. DOD will continue to expand companies' participation in threat information sharing programs, such as the Cyber Security/Information Assurance program.

c. As the certification authority for DIB cleared defense contractor sites, the Defense Security Service will expand education and training programs to include material for DOD personnel and DIB contractors to enhance their cyber threat awareness.

d. In addition, the Office of the Under Secretary of Defense for Intelligence will review the sufficiency of current classification guidance for critical acquisition and technology programs to protect information on contractor networks.[112]

7. **Private Industry**. Many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively. Therefore, DOD will work with the DHS, other interagency partners, and the private sector to improve cybersecurity. One example of such cooperation is the 2010 memorandum of agreement signed by DOD and DHS to align and enhance cybersecurity collaboration. The memorandum formalizes joint participation in program planning

and improves a shared understanding of cybersecurity. Under this memorandum USCYBERCOM and DHS exchange liaison personnel. DOD supports DHS in leading interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. DOD will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the information and communications technology (ICT) sector. The global technology supply chain affects mission critical aspects of the DOD enterprise and IT risks must be mitigated through strategic public-private sector cooperation.[113]

V. Department of Homeland Security Cyberspace Responsibilities

1. DHS has the responsibility to secure cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace intrusions and attacks. The DOD ensures secure operation of the DOD portion of cyberspace and depends on other USG departments and agencies to secure the portions of cyberspace under their authority.

2. Within DHS, the National Cyber Security Division (NCSD) is tasked to protect the USG network systems from cyberspace threats. NCSD partners with government, industry, and academia, as well as the international community, to make cybersecurity a national priority and to reinforce that cybersecurity is a shared responsibility.

3. The National Security Presidential Directive 54/Homeland Security Presidential Directive 23, issued on 2 Jan 2008, established the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI formalizes a series of continuous efforts to further safeguard Federal systems from cyberspace threats. Under the CNCI, DHS has the lead in a number of areas, to include:

a. Establish a frontline defense to reduce current vulnerabilities and prevent intrusions.

b. Defend against the full spectrum of threats by using intelligence and strengthening supply chain security.[114]

This Page Intentionally Blank

Chapter 6: Cyberspace Operations – Case Study

I. Russian Operations against Georgia in 2008

1. **Scenario**. Russia used cyberspace missions and actions in concert with other instruments of national power to achieve success in their operation against Georgia in 2008. This case study provides an opportunity to apply the principles outlined in this guide to a real-world event (see Figure 6-1).

Figure 6-1: Russian – Georgian Conflict, August 2008[115]

a. **Cross-Domain Synergy**. The war between Georgia, Russia, and the Russian-backed self-proclaimed republics of South Ossetia and Abkhazia saw some 35,000-40,000 Russian and allied forces, augmented by significant air and naval forces, confront some 12,000-15,000 Georgian forces with little air and minimal naval capability. Although a short and limited conflict, it was historic and precedent setting. This appears to be the first coordinated cyberspace attack synchronized with major combat actions in the other warfighting domains, primarily land and air.

b. **Cyberspace Intelligence Collection**. Russian cyberspace operations began several weeks before the outbreak of kinetic operations. Russian cyber intelligence units conducted reconnaissance on important sites and infiltrated Georgian military and government networks in search of data useful for the upcoming campaign. During this period, the Russian government began organizing the work of Russian cyberspace militias - irregular hackers outside the government - that would support the campaign and provide cover for some of the government's operations. Russian government and cyberspace militias conducted rehearsals of attacks against Georgian targets.

c. **DCO Response Actions (DCO-RA)**. Russian forces also attacked Georgian hacker forums in order to pre-empt a retaliatory response against Russian cyberspace targets.

d. **Deny – Degrade**. Russian cyberspace forces attacked civilian sites near the action of kinetic operations with the goal of creating panic in the civilian population. For example, in the town of Gori, Russians disabled government and news websites with DDoS attacks just prior to an air attack. Cyberspace interdiction (attacks concentrated on tactical data links and data fusion centers) degraded and disrupted the Georgians' decision cycle limiting their military response.

e. **Deny – Disrupt**. The Russian cyberspace operations forces disrupted Georgian government, military, and diplomatic communications.

(1) **Government and military communications**. When the kinetic battle started on 7 August, Russian government and irregular forces conducted distributed denial-of-service (DDoS) attacks on Georgian government and military websites. These attacks disrupted the transmission of information between military units and between offices in the Georgian government.

(2) **International communications**. Faced by overwhelming Russian air power, armored attacks on several fronts, an amphibious assault on its Black Sea coastline, and devastating cyber-attacks, Georgia had little capability of kinetic resistance. Its best hope lay with strategic communications: transmitting to the world a sympathetic message of rough treatment at the hands of Russian military aggression. But Russia effectively used cyberspace operations to disrupt the Georgian government's ability to assemble and transmit such a plea thus removing Georgia's last hope for international support.

f. **Deny – Destroy (potential)**. The Russians were very sophisticated in their target selection. For example, Russians refrained from attacking Georgia's most important asset, the Baku-Ceyhan oil pipeline and associated infrastructure. By holding this target in reserve, the Russians gave Georgian policymakers an incentive to quickly end the war.

g. **Manipulate**. Although there were no know attempts to manipulate data, the Russian cyberspace operations forces dislocated Georgian data flows, shunting data that normally would have traveled over the Internet into more traditional conduits such as telephone and radio communications. Georgians were trying to transmit more data at a higher rate than the useful capacity of their information network could accommodate because a large proportion was being consumed by cyber attacks injecting extraneous data into the network. The cyber attacks effectively jammed Georgia’s overall information network during the early stages of the war when rapid and organized action by Georgian defenses, cyber and kinetic, could have had the greatest impact.[116]

h. In summary, Russian planners tightly integrated cyberspace operations with their diplomatic, information, military, and economic elements of power (i.e. DIME). The Russo-Georgian war provides a case study for joint planners preparing for a future conflict, involving the new domain of cyberspace.[117]

II. Russian Cyberspace Operations Design, Planning, and Execution

1. **Cyberspace Operations Team**. This section demonstrates notional cyberspace operations team design, planning, and execution activities in support of the Russian operation in Georgia.

2. **Cyberspace Design Activities**. The design principles outlined in this handbook provide a guide for a cyberspace operations team to assist the commander in developing an operational approach for this scenario.

a. **Understanding the Cyberspace Environment**. After receiving direction to plan the operation, the cyberspace operations team attempts to gain an understanding of the operational environment. The CO team studies the Georgian, Russian, and international environment with a focus on physical and logical networks as well as key individuals and groups (see Figure 6-2).

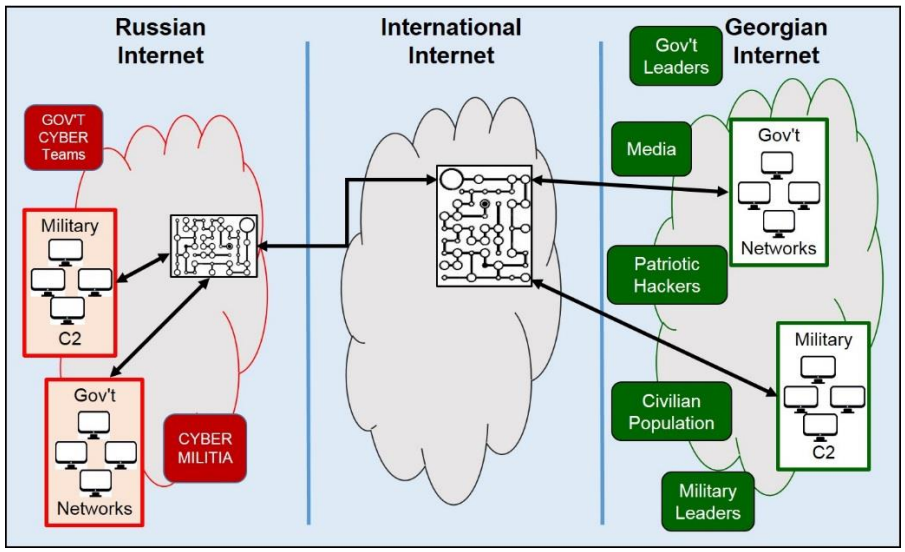

Figure 6-2: Georgian, Russian, and International Cyberspace Environment
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

b. **Understanding the Problem(s) in Cyberspace**. After identifying key individuals, groups, and physical and logical networks, the CO team focuses on identifying and understanding the problem(s) associated with the operation. The team identifies cyberspace challenges, threats, and risks to operations. They attempt to understand the adversary's resiliency and recovery capabilities. A recurrent cyberspace operations risk is losing anonymity.

c. **Developing the Operational Approach**. The operational approach is the commander's visualization of how the operation should transform current conditions into the desired conditions at end state. When developing an operational approach, a commander should synchronize actions '*in*' and '*through*' cyberspace with other activities to achieve the desired objectives. The commander can use lines of operation (LOOs) and lines of effort (LOEs) to show how the objectives will be achieved (see Figure 6-3).

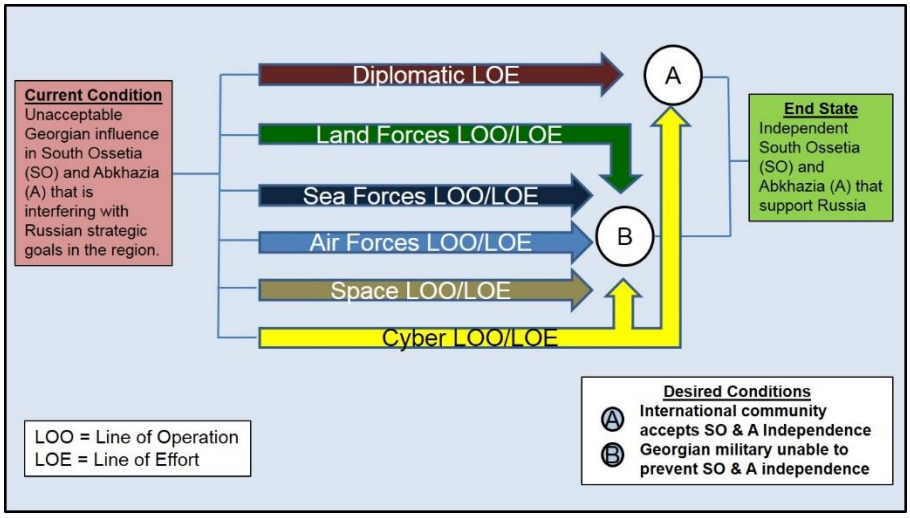

Figure 6-3: Russian Operational Approach in Georgia
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

3. **Cyberspace Planning Activities**. Planning translates strategic guidance and direction into campaign plans and operation orders. Based on the commander's operational approach and guidance, the CO team will assist the staff in developing and analyzing courses of action and developing the plan or order. The team should further develop and phase CO LOOs/LOEs for inclusion in the Cyberspace Operations Concept (see Figure 6-4).

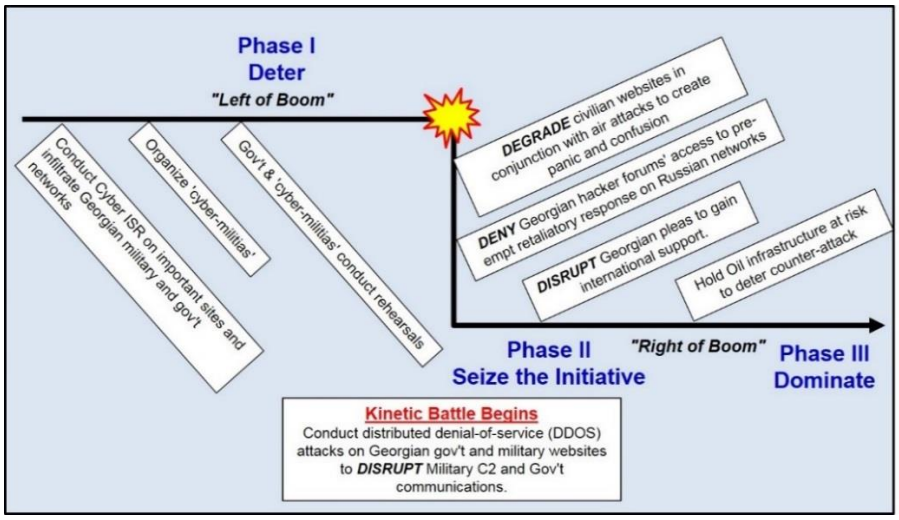

Figure 6-4: Russian Cyberspace Operations Concept in Georgia
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

4. **Cyberspace Operations during Execution**. Planning continues during execution, with an initial emphasis on refining the existing plan and producing the Operation Order (OPORD) and refining the force flow utilizing assigned and allocated forces. During execution, the CO team supports future plans, future operations, and current operations.

a. **Cyberspace Enabled Effects**. Cyberspace planners should focus their efforts on conducting cyberspace actions that achieve the commander's objectives. Cyberspace Operations planners should be concerned with the accumulation of tactical effects into an overall operational effect. At the operational level, objectives and desired effects are developed by the commander's staff and are used to develop tasks to subordinates. In this scenario, the Russian CO teams defended their networks and ensured anonymity while employing DDOS and other techniques to deny the Georgian government and military the ability to effectively respond. These cyberspace effects directly contributed to the accomplishment of the commander's objectives and end state (see Figure 6-5).

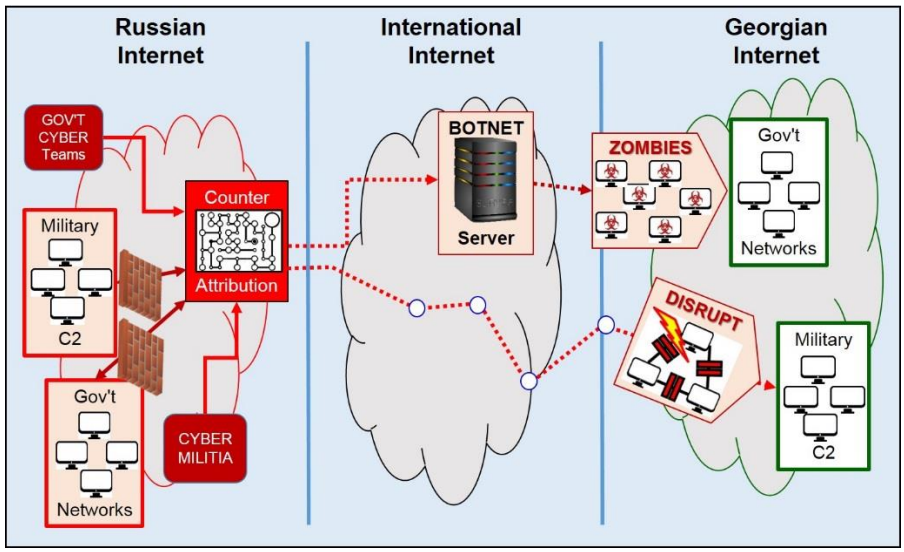

Figure 6-5: Russian Cyberspace Enabled Effects
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

b. **Target Development - Lead Time**. It's critically important to start cyberspace operations planning early. The lead time necessary to generate intelligence for the offensive cyberspace operations often takes longer than that required for kinetic operations. Target development should be requested much earlier than that for a traditional targets and should have a longer-term focus. In this scenario, Russian cyber intelligence units conducted reconnaissance on important sites and infiltrated Georgian military and government networks in search of data useful for the upcoming campaign. The cyberspace teams also conducted rehearsals prior to execution.

c. **Targeting Coordination and Authorization**. Cyberspace targets require detailed joint, cross-Combatant Command, interagency, and likely multinational planning and coordination, engagement, assessment, and intelligence efforts. The actual prosecution of a targets through cyberspace requires that cyberspace planners and operators coordinate with the supported commander early in the planning phase to ensure access to the target is available when the fleeting opportunity arises. In addition, commanders should establish procedures to quickly promulgate execution orders (EXORDs) for CO-engaged targets, which due to their unique cyberspace interagency deconfliction/coordination requirements may involve coordinating pre-approval for specific actions conducted under specific circumstances.

III. Georgian Defensive Cyberspace Operations

1. Russian cyberspace operations teams maintained cyber superiority throughout the conflict, and as a result Georgia never mounted a successful cyber defense or cyber counterattack. This was due in a large part to a critical cyber vulnerability—more than half of Georgia's 13 connections to the outside world via the Internet passed through Russia, and most of the Internet traffic to Web sites within Georgia was routed through Turkish or Azerbaijani Internet service providers, many of which were in turn routed through Russia. Overall, the cyber defense efforts were too little too late.[118] This section will demonstrate defensive cyberspace operations planning and actions that Georgian cyberspace operations teams attempted to use to mitigate the severity of Russian offensive cyberspace operations (see Figure 6-6).

a. **Defense Network Operations**. Despite their lack of success, the Georgian Cyberspace Operations teams attempted to conduct information network operations

(similar to Department of Defense Information Network Operations) to enhance the security of their military networks. They monitored the flow of information over their information networks. The Georgian CO team also attempted proactive actions which addressed their entire defense network, including configuration control and patching, cybersecurity measures and user training, physical security and secure architecture design, intrusion detection, bandwidth management/spectrum management, operation of host-based security systems and firewalls, and encryption of data.[119]

b. **Defensive Cyberspace Operations (DCO)**. The Georgian CO teams conducted passive and active defense cyberspace operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

(1) **DCO Internal Defensive Measures (DCO-IDM)**. The CO teams used internal defensive measures within their networks. These measures included actively hunting for advanced internal threats as well as the internal responses to these threats.[120] For example, Georgia attempted to maneuver around the cyber attacks by filtering them out based on their origin. However, the Russian cyber attackers' intelligence preparation allowed them to easily defeat this tactic. The Russian attackers routed their assault through foreign servers to mask their real IP addresses and created false IP addresses to spoof Georgia's cyber defense filters. Still, the Georgian CO teams preserved the use of some government web sites by moving them to U.S.-based servers.[121]

(2) **DCO Response Actions (DCO-RA)**. The Georgian CO teams also conducted limited DCO-RA to counter the Russian government cyberspace operations teams and 'cyber militias'. These actions were taken external to the defense network to defeat ongoing or imminent threats in order to defend their defense cyberspace capabilities. The CO teams attempted at least one major counterattack, but it failed. They posted cyber attack tools and instructions in Russian-language Internet forums to deceive pro-Russian cyber forces into unwittingly attacking Russian Web sites. This Georgian counterattack appears to have had a negligible effect on the Russian Web sites targeted.[122]

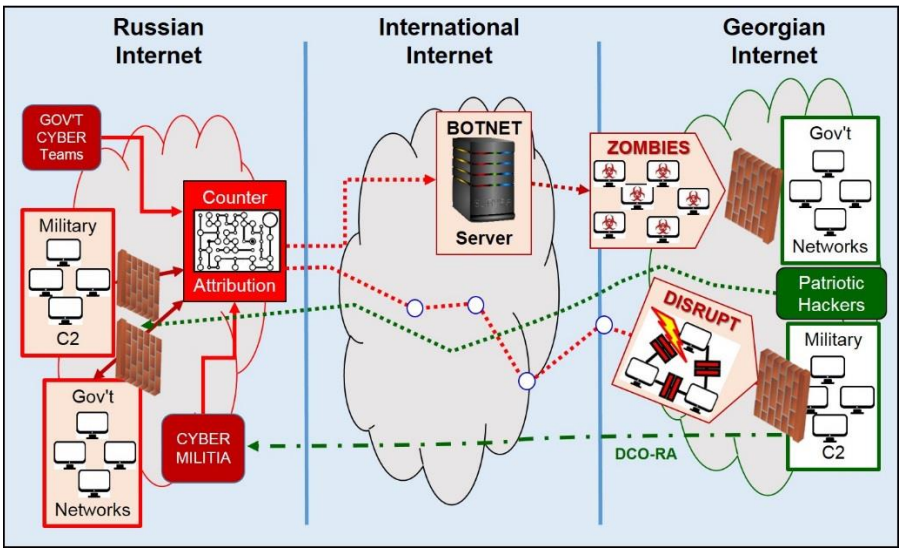

Figure 6-6: Georgian Defensive Cyberspace Operations (DCO)
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

Appendix A: U.S. Strategies, Guidance, and Doctrine

Appendix A includes:

I. National Strategy and Guidance

- **U.S. International Strategy for Cyberspace**
- **Framework for Improving Critical Infrastructure Cybersecurity**
- **The Cybersecurity Strategy for the Homeland Security Enterprise**

II. Department of State Policy Statements

- **Secretary of State Speech**
- **DOS Legal Opinion**

III. Department of Defense Strategy and Guidance

- **DOD Strategy for Operating in Cyberspace**
- **DOD Law of War Manual**

IV. Joint and Service Doctrine

- **Joint Cyber Doctrine**
- **Army Cyber Doctrine**
- **Marine Corps Cyber Doctrine**
- **Navy Cyber Doctrine**
- **Air Force Cyber Doctrine**

I. National Strategy and Guidance

A. U.S. International Strategy for Cyberspace

This factsheet provides an overview of the International Strategy for Cyberspace released by The White House on 16 May 2011. The full strategy can be found at: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

INTERNATIONAL STRATEGY FOR CYBERSPACE
Prosperity, Security, and Openness in a Networked World

The U.S. International Strategy for Cyberspace outlines our vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize it.

We live in a rare historical moment with an opportunity to build on cyberspace's successes and help secure its future—for the United States, and the global community.

Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. The reach of networked technology is pervasive and global. To realize fully the benefits that networked technology promises the world, these systems must function reliably and securely. Assuring the free flow of information, the security and privacy of data, and the integrity of the interconnected networks themselves are all essential to American and global economic prosperity, security, and the promotion of universal rights.

Strategic Approach

The United States' approach to international cyberspace issues is founded on the belief that networked technologies hold immense potential for our Nation, and for the world. The United States will pursue an international cyberspace policy that stokes the innovation that drives our economy and improves lives here and abroad.

Our strategic approach builds on successes, recognizes the challenges to our national and economic security, and is always grounded by our unshakable commitments to fundamental freedoms of expression and association, privacy, and the free flow of information.

The Future We Seek

The cyberspace environment that we seek rewards innovation and empowers entrepreneurs; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. This cyberspace is defined by four key characteristics:

- **Open** to innovation
- **Interoperable** the world over
- **Secure** enough to earn people's trust
- **Reliable** enough to support their work

To realize this vision, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law. These norms include:

- Upholding Fundamental Freedoms
- Respect for Property
- Valuing Privacy
- Protection from Crime
- Right of Self-Defense
- Global Interoperability
- Network Stability
- Reliable Access
- Multi-stakeholder Governance
- Cybersecurity Due Diligence

To realize this future, the United States will combine *diplomacy*, *defense*, and *development* to enhance prosperity, security, and openness so all can benefit from networked technology.

Diplomacy: Strengthening Partnerships

The United States will work to create incentives for, and build consensus around, an international environment in which states – recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace – work together and act as responsible stakeholders. Through our international relationships and affiliations, we will seek to ensure that as many stakeholders as possible are included in this vision of cyberspace precisely because of its economic, social, political, and security benefits.

Distributed systems require unified action because no single institution, document, arrangement, or instrument could suffice in addressing the needs of our networked world. From end-users, private- sector hardware and software vendors, and Internet service providers, to regional, multilateral, and multi-stakeholder organizations – all are important in helping cyberspace meet its full potential.

Defense: Dissuading and Deterring

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, thereby dissuading and deterring malicious actors, while reserving the right to defend these vital national assets as necessary and appropriate. The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

Development: Building Prosperity and Security

We believe the benefits of a connected world are universal. The virtues of an open, interoperable, secure, and reliable cyberspace should be more available than they are today, and as the world's leading information economy, the United States is committed to ensuring others benefit from our technical resources and expertise.

Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems. The United States' capacity-building assistance is envisioned as an investment, a commitment, and an important opportunity for dialogue and partnership. As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity- building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern.

Policy Priorities

This strategy is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. It is a call to the private sector, civil society, and end- users to reinforce these efforts through partnership, awareness, and action. It is also a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation.

The United States Government organizes its activities across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector. Taken as a whole, they form the action lines of our strategic framework.

Economy: Promoting International Standards and Innovative, Open Markets

To ensure that cyberspace continues to serve the needs of our economies and innovators, we will:

- Sustain a free-trade environment that encourages technological innovation on accessible, globally linked networks.
- Protect intellectual property, including commercial trade secrets, from theft.
- Ensure the primacy of interoperable and secure technical standards, determined by technical experts.
- Protecting Our Networks: Enhancing Security, Reliability, and Resiliency
- Because strong cybersecurity is critical to national and economic security in the broadest sense, we will:
- Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships.
- Reduce intrusions into and disruptions of U.S. networks.
- Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure.
- Improve the security of the high-tech supply chain, in consultation with industry.

Law Enforcement: Extending Collaboration and the Rule of Law

To enhance confidence in cyberspace and pursue those who would exploit online systems, we will:

- Participate fully in international cybercrime policy development.
- Harmonize cybercrime laws internationally by expanding accession to the Budapest
- Convention.
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet.
- Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.
- Military: Preparing for 21st Century Security Challenges

- Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:
- Recognize and adapt to the military's increasing need for reliable and secure networks.
- Build and enhance existing military alliances to confront potential threats in cyberspace.
- Expand cyberspace cooperation with allies and partners to increase collective security.

Internet Governance: Promoting Effective and Inclusive Structures
To promote Internet governance structures that effectively serve the needs of all Internet users, we will:

- Prioritize openness and innovation on the Internet.
- Preserve global network security and stability, including the domain name system (DNS).
- Promote and enhance multi-stakeholder venues for the discussion of Internet Governance issues.
- International Development: Building Capacity, Security, and Prosperity
- To promote the benefits of networked technology globally, enhance the reliability of our shared networks, and build the community of responsible stakeholders in cyberspace, we will:
- Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity.
- Continually develop and regularly share international cybersecurity best practices.
- Enhance states' ability to fight cybercrime – including training for law enforcement, forensic specialists, jurists, and legislators.
- Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Government counterparts.

Internet Freedom: Supporting Fundamental Freedoms and Privacy
To help secure fundamental freedoms as well as privacy in cyberspace, we will:

- Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.
- Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions.
- Encourage international cooperation for effective commercial data privacy protections.
- Ensure the end-to-end interoperability of an Internet accessible to all.

These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

Source:
https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf, accessed 17 May 2016.

B. Framework for Improving Critical Infrastructure Cybersecurity

The National Institute of Standards and Technology released this framework on 12 February 2014. The following is an excerpt of the Executive Summary, The full document can be found at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use of this voluntary Framework is the next step to improve the cybersecurity of our Nation's critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole.

Source: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, accessed 17 May 2016.

C. The Cybersecurity Strategy for the Homeland Security Enterprise

Department of Homeland Security (DHS) released this strategy in November 2011. It was developed pursuant to the Quadrennial Homeland Security Review and reflects the importance of cyberspace to our economy, security, and way of life. The following is an excerpt of the Executive Summary, The full document can be found at: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

Executive Summary

The Blueprint for a Secure Cyber Future builds on the Department of Homeland Security Quadrennial Homeland Security Review Report's strategic framework by providing a clear path to create a safe, secure, and resilient cyber environment for the homeland security enterprise. With this guide, stakeholders at all levels of government, the private sector, and our international partners can work together to develop the cybersecurity capabilities that are key to our economy, national security, and public health and safety. The Blueprint describes two areas of action: Protecting our Critical Information Infrastructure Today and Building a Stronger Cyber Ecosystem for Tomorrow. The Blueprint is designed to protect our most vital systems and assets and, over time, drive fundamental change in the way people and devices work together to secure cyberspace. The integration of privacy and civil liberties protections into the Department's cybersecurity activities is fundamental to safeguarding and securing cyberspace.

The Blueprint lists four goals for protecting critical information infrastructure:

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

These goals are supported by nine objectives. Each objective is dependent on a variety of capabilities that, when implemented, will work in tandem to effectively anticipate and respond to a wide range of threats. Some of the cybersecurity capabilities described in the Blueprint are robust and at work today, while others must be expanded. Still others require further research and development. All necessitate a collaborative and responsive cybersecurity community.

Achieving a safe, secure, and resilient cyber environment includes measuring progress in building capabilities and determining whether they are effective in an evolving threat environment. Accordingly, each year's performance will be compared with that of the previous year. This approach will highlight where progress is being made and will identify gaps and resource requirements.

Cyberspace underpins almost every facet of American life, and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. Protecting cyberspace requires strong vision, leadership, and a broadly distributed effort in which all members of the homeland security enterprise take responsibility. The Blueprint for a Secure Cyber Future was developed to address this reality.

Source: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf, accessed 17 May 2016.

II. Department of State Policy Statements

A. Secretary of State Speech on Internet Security

An Open and Secure Internet: We Must Have Both

The following speech by John Kerry, Secretary of State, was made at Korea University in Seoul, South Korea on 18 May 2015 and is posted on the DOS website: http://www.state.gov/secretary/remarks/2015/05/242553.htm.

SECRETARY KERRY: (Applause.) Well, good afternoon, President Yeom. Thank you very much for a generous introduction. Distinguished guests, all, I'm delighted to be here and I want to thank the university, and particularly Park No-young, the Director of the Cyber Law Center, for inviting me to be here today. Thank you very, very much.

I also want to acknowledge somewhere – I don't see him – but my friend, the ambassador from the United States of America – there he is right in front of me – Mark Lippert, who represents the United States here in Seoul. And he's a special person. I've known him for a long time. He served in the United States Navy. He served in Afghanistan and served for the President, been an advisor to several presidents. But recently, as you all know, he displayed great grace and dignity under duress, and like all of our diplomats, whose jobs carry with them certain risks on the front lines of diplomacy, I will tell you that Mark has never wavered from his determination to do his job and to represent our country to the best of his ability – which, believe me, he does. So I'm grateful for his leadership. And, Mark, thank you for the great example you're setting.

I'm really happy to be back here in Seoul. This is a beautiful city, and I'm struck every time I come here. I wish I had more time. Time is the enemy of those of us in diplomacy nowadays. But the United States and South Korea share a very special history, obviously, and we also share great hopes for the future. And I am very happy to be here to talk about our shared interests, though it will not just be, President Yeom, about the security; it will be about the internet itself, which is important as we think about security. It's also, obviously, very critical as we think about the many interests that we share together, ranging from security on the Korean Peninsula, to the success of the Korea-U.S. Free Trade Agreement, to the many connections that exist between the Korean and the American peoples – including, I want you to know, a love for Psy, K-Pop, bibimbap, and Pororo, the little penguin. (Laughter.) I want you to know that my staff recommended that I walk out here this afternoon, dancing to Gangnam Style – but I told them no, that's too 2012.

Today, it's really more than appropriate to be here in the most wired city in the country, one of the most wired cities in the world, in order to speak with you about digital technology and about the fears and the possibilities that we associate with digital technology. And let me underscore: It's the possibilities that should motivate us, and it's the possibilities that bring me here today.

Now, years ago, South Korea made a conscious choice to become a global IT leader and you have delivered. As a society, you opened the door to investment, you encouraged households to sign up for broadband, you eased the transition to new technology, and you developed programs in universities just like this one to educate young people in digital skills. And I applaud you for the remarkable linkage to the military and the security side of it with the offer that you make to students who will come here, learn, and then go on to serve the country in the military for those seven years.

Today, thanks in part to President Park's commitment to build a, quote, "creative economy," the ROK is a virtual synonym for Internet success stories, such as the educational network service ClassTing; or the Kakao, your messenger app which is one of the fastest-growing tech firms in all of Asia; and GRobotics, a company which has revolutionized the robot industry and,

incredibly, it was originally conceived by an amazing 11-year-old child. Just two weeks ago, Ambassador Lippert joined President Park at the opening of the Google Campus for startups and entrepreneurs right here in Seoul – an initiative designed to spur the exchange of ideas and digital growth in both of our countries. Now, both of our nations know and view the internet and cyber issues as part of a new frontier for our governments and peoples, and it will be one of the key areas discussed when our two presidents meet in in Washington in June.

The fact is, whichever side of the Pacific Ocean we live on, the internet today is part of almost everything that we do. And just to tell you how amazing it is, I served in the United States Senate on the Commerce Committee in 1996. I was chairman of the Communications Subcommittee when we rewrote the communications law for our country. And guess what? Barely anybody in 1996 was talking about data, and data transformation, and data management. It was all about telephony – the telephone. That's how far we've traveled in 20 years.

So it matters to all of us how the technology is used and how it's governed. That is precisely why the United States considers the promotion of an open and secure internet to be a key component of our foreign policy. It's why we want to work with you and with international partners everywhere in order to better understand the choices that we face in managing this extraordinary resource – a resource which does present us with certain challenges even as it presents us with unprecedented opportunities.

Now, what do I mean by that?

Well, to begin with, America believes – as I know you do – that the internet should be open and accessible to everyone. We believe it should be interoperable, so it can connect seamlessly across international borders. We believe people are entitled to the same rights of free expression online as they possess offline. We believe countries should work together to deter and respond effectively to online threats. And we believe digital policy should seek to fulfill the technology's potential as a vehicle for global stability and sustained economic development; as an innovative way to enhance the transparency of governments and hold governments accountable; and also as a means for social empowerment that is also the most democratic form of public expression ever invented.

At its best, the internet is an equal-opportunity platform from which the voice of a student can have as much reach as that of a billionaire; a chief executive may be able to be out-debated by an entry-level employee – and there's nothing wrong with that. Most users of the internet agree, on the internet as in any other venue, the human rights of every person – including freedom of expression – should be protected and respected. The United Nations has repeatedly affirmed this view, but as we know, it is still not universally held. That means that we will continue to have important choices to make – important choices to make locally, to make in universities, to make in businesses, to make in countries, and between countries. We will have a lot of choices about technology among and between nations.

Let me tell you something: How we choose begins with what we believe. And what we believe about the internet hinges to a great extent on how we feel, each and every one of us, about freedom.

Freedom. The United States believes strongly in freedom – in freedom of expression, freedom of association, freedom of choice. But particularly, this is important with respect to freedom of expression, and you believe in that freedom of expression here in Korea. We want that right for ourselves and we want that right for others even if we don't agree always with the views that others express. We understand that freedom of expression is not a license to incite imminent violence. It's not a license to commit fraud. It's not a license to indulge in libel, or sexually exploit

children. No. But we do know that some governments will use any excuse that they can find to silence their critics and that those governments have responded to the rise of the internet by stepping up their own efforts to control what people read, see, write, and say.

This is truly a point of separation in our era – now, in the 21st century. It's a point of separation between governments that want the internet to serve their citizens and those who seek to use or restrict access to the internet in order to control their citizens.

Here in the Asia Pacific, we see countries such as the ROK and Japan that are among the world's leaders in internet access, while North Korea is at the exact opposite end of that spectrum, with the lowest rate of access in the world and the most rigid and centralized control.

No other government is as extreme as the DPRK, but there are more than a few who want to harvest the economic benefits of the internet while nevertheless closing off the avenues of political, social, and religious expression. They impose filters that eliminate broad categories of what their citizens can see and receive and transmit – and with whom ideas may be changed and shared. What's more, the governments that have pioneered the repressive use of such technologies are quick to export their tools and methods to others, and thereby further diminish individual rights. At the same time, some governments are using the internet to track down activists and journalists who write something that they don't like, and even reach beyond their borders in order to intimidate their critics.

My friends, this discourages free expression and it clearly seems intended to turn their part of the internet into a graveyard for new ideas – the exact opposite of what it should be, a fertile field where such ideas can blossom and grow.

Let's be clear: Every government has a responsibility to provide security for its citizens. Yes. We all agree with that. In the United States, our efforts to do so – and the reforms that we have undertaken in the process – have been guided by our concern for individual rights and our commitment to oversight and review. Further, unlike many, we have taken steps to respect and safeguard the privacy of the citizens of other countries and to use the information that we do collect solely to address the very specific threat to the United States and to our allies. We don't use security concerns as an excuse to suppress criticisms of our policies or to give a competitive advantage to an American company and any commercial interests at all.

Now, regrettably, it is no coincidence that many of the governments that have a poor record on internet freedom also have a questionable commitment to human rights more generally. United States policy has always been to engage with such governments to encourage reforms and to point out the contributions to prosperity that would flow from a more open approach. Regimes that practice repression typically argue that they have no obligation to justify what they do inside their own borders, but that assertion is directly contradicted by the Universal Declaration of Human Rights and by many other multilateral declarations and statements.

The fact is, an individual's aspiration to be free may be the most single powerful force on Earth. It's an aspiration that may be able to be slowed sometimes, maybe intimidated sometimes, it may even be eliminated temporarily by violence in certain cases. But I'm telling you its power within the human soul is so infectious that it will always resurface in one form or another, even in the most extraordinary circumstances.

And history – history has proven that again and again and again. Throughout history, we have seen that men and women will do whatever it takes to find a way to make their desire for freedom known. We saw that with the authors of the pamphlets that helped to spark the revolution that gave birth to my home country in the 1700s. We saw it with the dissidents writing newsletters and producing radio broadcasts behind the Iron Curtain during the Cold War. And

we see it today, in places all over the world, where young people are challenging injustice – armed only with their smart phones.

The internet is, among many other things, an instrument of freedom. It's a tool people resort to in response to the absence and failure or abuse of government. So of course, some leaders are afraid of it. They're afraid of the internet in the same way that their predecessors were afraid of newspapers, books, and the radio, but even more so because in this case, because of the interactivity that allows for a free-flowing discussion and the exchange of views – activities that can, and often do, lead to change.

I say to you today, here at Korea University, that fear is misplaced, and that response is, in the end, futile. Anyone who blames the internet for the disorder or turmoil in today's world is just not using their head to connect the dots correctly. And banning the internet in a misguided attempt to impose order will never succeed in quashing the universal desire for freedom.

Ladies and gentlemen, repression does not eliminate the speech we hate. It just forces it into other avenues – avenues that often can become more dangerous than the speech itself that people are fighting. The remedy for the speech that we do not like is more speech. It's the credible voices of real people that must not only be enabled, but they need to be amplified.

The good news is that much of the world understands this. More and more of the world understands this. And the advocates of internet freedom and openness are speaking up. The United States is part of the Freedom Online Coalition, a 26-country group that we are actively seeking to expand. The coalition argues that narrow and distorted visions of the internet cannot be allowed to prevail. Freedom must win out over censorship. That is an important principle, but it is also a practical imperative. After all, from the dawn of history to the present day, repression hasn't invented a thing. Freedom is how jobs are created, diseases are cured, alternative energy is harnessed, and new ways are found to feed a global population that has quadrupled in the past century and that will rise to some 9 billion people in the next 40 to 50 years. Without freedom, civilization can't advance; it's like a bicycle without pedals.

Remember that the internet is not just another sector of our economy. Like electricity, it is a general purpose technology that is used in thousands of different ways, streamlining everything from buying a cup of coffee to building a skyscraper. Consider what would happen if someone tried to block the flow of electricity – the lights would go out and everything would stop. In fact, when I was a lot younger, Hollywood made a movie about exactly that; it was called "The Day the Earth Stood Still." And thank heavens they made a couple more of them so you can't tell exactly which one I'm referring to. (Laughter.) Now, you might want to watch it, because policies that restrict online data streams have a similar effect, if perhaps not quite so dramatic.

Think, for example, of what would take place if every country imposed data localization requirements, causing information to halt and to undergo inspection whenever it reached a national border. Imagine what would happen to commerce and to the flow of information, to the simple effort to get an answer to a question at a dinner table when you're talking with people and you want to Google something. The delays would create huge obstacles to multinational business at a time when speed is of the essence and cross-border enterprises are major engines of growth. That's not a formula for progress; it's a way to stop progress in its tracks.

The internet provides broadly-shared connections that are essential for modern economies to be able to grow. It's that simple. It can help people even in remote areas take advantage of government services and make a better business decision, for example. Let me give you an example. It could make a difference to people about when you bring your crops to the market or how do you find international customers for local projects.

With digital technology, fishermen in Mozambique can keep their catch fresh in the water until they have a buyer, somewhere in another continent maybe, thus eliminating spoilage and waste.

Shopkeepers in sub-Saharan Africa have seen their incomes actually grow by using mobile banking technology to avoid local loan sharks and go directly to reputable financial institutions for emergency credit and loans.

The system becomes more accountable and more transparent and more accessible. Women entrepreneurs in Southeast Asia have formed cooperatives online that enable them to take advantage of economies of scale.

Children from Angola to India are learning more and faster through education that comes to them over the internet.

And a couple of years ago, a young engineer from Cameroon developed a computer tablet called "Cardiopad" that enables Africans to be able to have a heart examination at home and receive the diagnosis from doctors who may be hundreds of miles away. Think about that.

The examples are endless, but you get the point. I know. The internet fuels innovation that can lead to improved efficiency, improved productivity in every sector of a developing economy.

But in thinking about the internet's promise, you have to recognize how far that potential is from being fulfilled today. Roughly three out of every five people in the world today remain without internet access – and in the poorest countries that figure can top 95 percent.

A big part of the reason is simply cost. Ask yourself: How much of your family's income do you pay for internet access? In America, the average is 1 or 2 percent. But a typical family in some countries have to pay 10 percent for entry-level mobile broadband and roughly four times that for fixed broadband. In other words, people with low incomes can't afford digital access. They need to earn more money. To break that circle of despair, we need to bring the costs down by getting public policies right – because money isn't the only barrier.

There's a reason why access is relatively high in Colombia but low in Venezuela. There's a reason why it's high in Malaysia but low in Cambodia; a reason why it's high in Rwanda but low in Ethiopia. Some governments do much more than others to facilitate access for people in poor or remote areas. And the starting point is for every country to have a clear and comprehensive national broadband plan that allows for private investment, encourages competition, removes bureaucratic obstacles, and takes full advantage of shared internet services at schools, libraries, community centers, and cafes.

That's why two years ago the United States helped create the Alliance for Affordable Internet. This broad coalition draws on expertise from governments, the private sector, and civil society to assist policy makers in expanding access while keeping prices low. It's the right goal, and I'll tell you, it's also a smart goal. According to one recent European study, tripling mobile broadband penetration levels across the developing world would provide a return of as much as $17 for every $1 spent.

About 10 days ago, when I was in Kenya, I Skyped, using the internet, with a group of young Somali refugees. Most of these refugees were high school or college age kids, and yet – and yet, extraordinarily, many of them had never, ever been outside that refugee camp – ever. This, in an era of incredible globalization – they had only lived in one refugee camp. The students I spoke to wanted desperately to be able to complete their schooling. They wanted to find a job. They wanted to go on to university. They wanted to begin a career. One young woman, who is studying chemistry and biology, told me she hoped to become a doctor. Now, I'm willing to bet you that she's never been inside a hospital. But that's what she wanted to do – become a

doctor. The irony is that, at the refugee camp, they have internet connections. Now, I can't help but wonder whether that will be the case when they return to Somalia.

If there is any message that is going to be sent to governments by young people in the world today, it is the desire – the universal desire – for jobs, for opportunity, for education, for a future. That's what people want. It's what every family in the world really wants. No one is asking to be censored. No one is yearning to be told what to think and how to live. The same desires that helped South Korea embrace democracy are what sparked the beginnings of the Arab Spring; they're what kept the pro-democracy movement alive through two decades of dictatorship in Burma; and they're what prompted the voters of Sri Lanka and Nigeria to flock to the polls in recent months and cast their ballots for change.

So looking to the future, we have to respond to this demand for openness and opportunity by making steady progress toward closing the digital divide. And with that goal in mind, the United States State Department will soon launch a new diplomatic initiative – in combination with partner countries, development banks, engineers, and industry leaders – and we're going to do just that: try to make it more available. You may be sure that we will be inviting your government and other representatives from this highly-connected country to help us lead and guide this effort. Because this will define the future. And this is the way we'll address violent extremism, and failing states.

So this brings me to another issue that should concern us all, and that is governance – because even a technology founded on freedom needs rules to be able to flourish and work properly. We understand that. Unlike many models of government that are basically top-down, the internet allows all stakeholders – the private sector, civil society, academics, engineers, and governments – to all have seats at the table. And this multi-stakeholder approach is embodied in a myriad of institutions that each day address internet issues and help digital technology to be able to function.

The versatility of the current approach enables it to move both with deliberation and care on complex issues and, frankly, much more rapidly on situations that demand a rapid response. For example, we saw the community respond to the 2007 cyberattacks in Estonia in a matter of hours. And as recently as last week, it responded literally in minutes to an unexpected outage of the Amsterdam exchange, which is the second-largest internet exchange point in the world.

That's why we have to be wary of those who claim that the system is broken or who advocate replacing it with a more centralized arrangement – where governments would have a monopoly on the decision-making. That's dangerous. Now, I don't know what you think, but I am confident that if we were to ask any large group of internet users anywhere in the world what their preferences are, the option "leave everything to the government" would be at the absolute bottom of the list. Because of the dynamic nature of this technology, new issues are constantly on the horizon – but the multi-stakeholder approach remains the fairest and the best, most effective way to be able to resolve those challenges.

Now, as everyone knows, it's impossible to talk about cyber policy without talking about international peace and security. You live this truth right here in South Korea, just as we do in the United States. Both of our countries have been hit by serious cyber-attacks from state and non-state actors. Worldwide, the risk and frequency of such attacks is on the increase.

America's policy is to promote international cyber stability. The goal is to create a climate in which all states are able to enjoy the benefits of cyberspace; all have incentives to cooperate and avoid conflict; and all have good reason not to disrupt or attack one another. To achieve this, we are seeking a broad consensus on where to draw the line between responsible and irresponsible behavior.

As I've mentioned, the basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties. We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace. We view these as universal concepts that should be appealing to all responsible states, and they are already gaining traction.

First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure. Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm. Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain. Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way. And fifth, every country should do what it can to help states that are victimized by a cyberattack.

I guarantee you if those five principles were genuinely and fully adopted and implemented by countries, we would be living in a far safer and far more confident cyberworld.

But even with these principles, ensuring international cyber stability will remain a work in progress. We still have a lot of work to do to develop a truly reliable framework – based on international law – that will effectively deter violations and minimize the danger of conflict.

To build trust, the UN Group of Governmental Experts has stressed the importance of high-level communication, transparency about national policies, dispute settlement mechanisms, and the timely sharing of information – all of them, very sound and important thoughts. The bottom line is that we who seek stability and peace in cyberspace should be clear about what we expect and intend, and those who may be tempted to cause trouble should be forewarned: they will be held accountable for their actions. The United States reserves the right to use all necessary means, including economic, trade and diplomatic tools, as appropriate in order to defend our nation and our partners, our friends, our allies. The sanctions against North Korean officials earlier this year are one example of the use of such a tool in response to DPRK's provocative, destabilizing and repressive actions, including the cyber-attack on Sony Pictures. Now, as the international community moves towards consensus about what exactly constitutes unacceptable behavior in cyberspace, more and more responsible nations need to join together to act against disruptors and rogue actors.

As we know, malicious governments are only part of the cybersecurity problem. Organized crime is active in cyberspace. So are individual con artists, unscrupulous hackers, and persons engaged in fraud. Unfortunately, the relative anonymity of the internet makes it an ideal vehicle for criminal activity – but not an excuse for working through the principles I described to finding rules of the road and working so that the internet works for everybody else. The resulting financial cost of those bad actors, the cost of cybercrime, is already enormous, but so is the loss of trust in the internet that every successful fraud or theft engenders.

And that's precisely why the United States is working with partners on every continent to strengthen the capacity of governments to prevent cyber-crime through improved training, the right legal frameworks, information sharing, and public involvement.

The best vehicle for international cooperation in this field is the Budapest Convention on Cybercrime, which my government urges every nation to consider joining. There is no better legal framework for working across borders to define what cybercrime is and how breaches of the law should be prevented and prosecuted. We also support the G-7 24/7 Network – in which

South Korea is an active participant – and that enables police and prosecutors from more than 70 countries to request rapid assistance on their investigations.

The United States is also working with partners to improve network defenses and in cooperation with other countries to respond to cyber incidents. All of this is crucial, because in an interconnected system like the internet, poor cybersecurity has the potential to increase the danger for all of us. So we have to help each other. We have to maintain direct contact between our incident response teams, invest heavily in that capacity, and build that capacity so that weak spots are turned into stronger blockages against the vulnerabilities, and ultimately, they disappear.

So to sum up, I think it is clear to all of us that the internet is not like most inventions that affect a single industry, require just a few tweaks – a little adjustment here and there – and then we can all move on. That's not what it requires. Digital technology has led us into a whole new frontier in which we have to find our way – and there are many different dimensions to it. When I was still in the United States Senate, I introduced legislation to protect the privacy rights of individuals and I still feel very strongly about that principle. And we are working to make sure we protect the privacy of people, not just in our country but in others.

As Secretary of State, I am in charge of an organization that is the target of hacking attempts every single day – and we have to defend against those. As a diplomat, I'm constantly engaged in discussions with counterparts about how to best enhance access and how to design and enforce the right rules to protect all of us.

My meetings with the private sector, the scientific community, the civil society, all bring home to me how important it is that all stakeholders have a voice in internet governance. The very essence of this technology is its freedom and its openness, and unless we bring all the stakeholders to the table, that will be lost. And something more important than all of us will be lost with it.

We cannot let that happen. Now, as I said before, obviously, the internet is not without risk – but at the end of the day, if we restricted all technology that could possibly be used for bad purposes, we'd have to revert to the Stone Age. Throughout the global community, we need to come together around principles that will establish a solid foundation for our freedoms – principles that will protect the rights of individuals, the privacy of our citizenry, and the security of our nations – all at the same time.

So I leave you with a somewhat unusual request: Keep doing what so many of you are already doing. Speak up for an open and secure internet. Defend freedom of expression. Add to South Korea's great reputation as a leader in digital technology. In doing so, we can be absolutely confident about the future that we will shape.

And how will we know when we finally have succeeded? When an open, secure internet is as widespread as electricity or cellphone coverage itself. When it is fully integrated into everyday life in every corner of the globe. When it is no longer contested but accepted and even taken for granted. When we reach that point – believe me: Your successors will look back at all of this debate and they will wonder how could anyone have argued the other way.

My friends, if we do all of these things, if we stick by our guns, the internet revolution that we are living today will literally define the kinds of opportunities that young people all over the world are hoping for today – help strengthen governments; provide opportunity; make us safer; bring us together; and in effect, define the future of this century. That's the goal we're fighting for, and we look forward to working with all of you to achieve it.

Source: http://www.state.gov/secretary/remarks/2015/05/242553.htm, accessed 17 May 2016.

B. DOS Position on International Law in Cyberspace

International Law in Cyberspace

The following presentation by Harold Hongju Koh, Legal Advisor U.S. Department of State, was made at the USCYBERCOM Inter-Agency Legal Conference in Ft. Meade, MD on 18 September 2012 and is posted on the DOS website: http://www.state.gov/s/l/releases/remarks/197924.htm.

As prepared for delivery

Thank you, Colonel Brown, for your kind invitation to speak here today at this very important conference on "the roles of cyber in national defense." I have been an international lawyer for more than thirty years, a government lawyer practicing international law for more than a decade, and the State Department's Legal Adviser for nearly 3 ½ years. While my daily workload covers many of the bread and butter issues of international law—diplomatic immunity, the law of the sea, international humanitarian law, treaty interpretation—like many of you, I find more and more of my time is spent grappling with the question of how international law applies in cyberspace.

Everyone here knows that cyberspace presents new opportunities and new challenges for the United States in every foreign policy realm, including national defense. But for international lawyers, it also presents cutting-edge issues of international law, which go to a very fundamental question: *how do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?*

Many, many international lawyers here in the U.S. Government and around the world have struggled with this question, so today I'd like to present an overview of how we in the U.S. Government have gone about meeting this challenge. At the outset, let me highlight that the entire endeavor of applying established international law to cyberspace is part of a broader international conversation. We are not alone in thinking about these questions; we are actively engaged with the rest of the international community, both bilaterally and multilaterally, on the subject of applying international law in cyberspace.

With your permission, I'd like to offer a series of questions and answers that illuminate where we are right now – in a place where we've made remarkable headway in a relatively short period of time, but are still finding new questions for each and every one we answer. In fact, the U.S. Government has been regularly sharing these thoughts with our international partners. Most of the points that follow we have not just agreed upon internally, but made diplomatically, in our submissions to the UN Group of Governmental Experts (GGE) that deals with information technology issues.

1. International Law in Cyberspace: What We Know

So let me start with the most fundamental questions:

Question 1: *Do established principles of international law apply to cyberspace?*

Answer 1: **Yes, international law principles do apply in cyberspace.** Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique

set of rules on cyberspace. But the United States has made clear our view that established principles of international law *do* apply in cyberspace.

Question 2: *Is cyberspace a law-free zone, where anything goes?*

Answer 2: **Emphatically no. Cyberspace is not a "law-free" zone where anyone can conduct hostile activities without rules or restraint.**

Think of it this way. This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law – international humanitarian law, or the law of armed conflict – affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation. To be sure, new technologies raise new issues and thus, new questions. Many of us in this room have struggled with such questions, and we will continue to do so over many years. But to those who say that established law is not up to the task, we must articulate and build consensus around how it applies and reassess from there whether and what additional understandings are needed. Developing common understandings about how these rules apply in the context of cyberactivities in armed conflict will promote stability in this area.

That consensus-building work brings me to some questions and answers we have offered to our international partners to explain how both the law of *going to* war (*jus ad bellum*) and the laws that apply in conducting war (*jus in bello*) apply to cyberaction:

Question 3: *Do cyber activities ever constitute a use of force?*

Answer 3: **Yes**. **Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.** In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.

Question 4: *May a State ever respond to a computer network attack by exercising a right of national self-defense?*

Answer 4: **Yes**. **A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.** As the United States affirmed in its 2011 International Strategy for Cyberspace, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."

Question 5: *Do jus in bello rules apply to computer network attacks?*

Answer 5: **Yes. In the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools. The principles of**

necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances. There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.

Question 6: *Must attacks distinguish between military and nonmilitary objectives?*

Answer 6: Yes. The *jus in bello* principle of distinction applies to computer network attacks undertaken in the context of an armed conflict. The principle of distinction applies to cyber activities that amount to an "attack" – as that term is understood in the law of war – in the context of an armed conflict. As in any form of armed conflict, the principle of distinction requires that the intended effect of the attack must be to harm a legitimate *military* target. We must distinguish military objectives – that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage – from civilian objects, which under international law are generally protected from attack.

Question 7: *Must attacks adhere to the principle of proportionality?*

Answer 7: **Yes. The *jus in bello* principle of proportionality applies to computer network attacks undertaken in the context of an armed conflict.** The principle of proportionality prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. Parties to an armed conflict must assess what the expected harm to civilians is likely to be, and weigh the risk of such collateral damage against the importance of the expected military advantage to be gained. In the cyber context, this rule requires parties to a conflict to assess: (1) the effects of cyber weapons on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians; (2) the potential physical damage that a cyber attack may cause, such as death or injury that may result from effects on critical infrastructure; and (3) the potential effects of a cyber attack on civilian objects that are *not* military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are military objectives.

Question 8: *How should States assess their cyber weapons?*

Answer 8: **States should undertake a legal review of weapons, including those that employ a cyber capability.** Such a review should entail an analysis, for example, of whether a particular capability would be *inherently indiscriminate*, *i.e.,* that it could not be used consistent with the principles of distinction and proportionality. The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict – first, an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.

Question 9: *In this analysis, what role does State sovereignty play?*

Answer 9: **States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict.** The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.

Question 10: *Are States responsible when cyber acts are undertaken through proxies?*

Answer 10: **Yes**. **States are legally responsible for activities undertaken through "proxy actors," who act on the State's instructions or under its direction or control.** The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for States in identifying, evaluating, and accurately responding to threats. But putting attribution problems aside for a moment, established international law does address the question of proxy actors. States are legally responsible for activities undertaken through putatively private actors, who act on the State's instructions or under its direction or control. If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful.

2. International Law in Cyberspace: Challenges and Uncertainties

These ten answers should give you a sense of how far we have come in doing what any good international lawyer does: applying established law to new facts, and explaining our positions to other interested lawyers. At the same time, there are obviously many more issues where the questions remain under discussion. Let me identify three particularly difficult questions that I don't intend to answer here today. Instead, my hope is to shed some light on some of the cutting-edge legal issues that we'll all be facing together over the next few years:

Unresolved Question 1: **How can a use of force regime take into account all of the novel kinds of *effects* that States can produce through the click of a button?**

As I said above, the United States has affirmed that established *jus ad bellum* rules do apply to uses of force in cyberspace. I have also noted some clear-cut cases where the physical effects of a hostile cyber action would be comparable to what a kinetic action could achieve: for example, a bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result. As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by "force." At the same time, the difficulty of reaching a definitive legal conclusion or consensus among States on when and under what circumstances a hostile cyber action would constitute an armed attack does not automatically suggest that we need an entirely new legal framework specific to cyberspace. Outside of the cyber-context, such ambiguities and differences of view have long existed among States.

To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response – such responses must still be *necessary* and of course *proportionate*. We recognize, on the other hand, that some other countries and commentators have drawn a distinction between the "use of force" and an "armed attack," and view "armed attack" – triggering the right to self-defense – as a subset of uses of force, which passes a higher threshold of gravity. My point here is not to rehash old debates, but to illustrate that States have long had to sort through complicated *jus ad bellum* questions. In this respect, the existence of complicated cyber questions relating to *jus ad bellum* is not in itself a new development; it is just applying old questions to the latest developments in technology.

Unresolved Question 2: **What do we do about "*dual-use* infrastructure" in cyberspace?**

As you all know, information and communications infrastructure is often shared between State militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack, including in the cyber realm. But how, exactly, are the *jus in bello* rules to be implemented in cyberspace? Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are *not* military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review. Any number of factual scenarios could arise, however, which will require a careful, fact-intensive legal analysis in each situation.

Unresolved Question 3: **How do we address the problem of *attribution* in cyberspace?**

As I mentioned earlier, cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability," by acting through proxies. I noted that legal tools exist to ensure that States are held accountable for those acts. What I want to highlight here is that many of these challenges – in particular, those concerning attribution – are as much questions of a technical and policy nature rather than exclusively or even predominantly questions of law. Cyberspace remains a new and dynamic operating environment, and we cannot expect that all answers to the new and confounding questions we face will be *legal* ones.

These questions about effects, dual use, and attribution are difficult legal and policy questions that existed long before the development of cyber tools, and that will continue to be a topic of discussion among our allies and partners as cyber tools develop. Of course, there remain many other difficult and important questions about the application of international law to activities in cyberspace – for example, about the implications of sovereignty and neutrality law, enforcement mechanisms, and the obligations of States concerning "hacktivists" operating from within their territory. While these are not questions that I can address in this brief speech, they are critically important questions on which international lawyers will focus intensely in the years to come.

And just as cyberspace presents challenging new issues for lawyers, it presents challenging new technical and policy issues. Not all of the issues I've mentioned are susceptible to clear legal answers derived from existing precedents – in many cases, quite the contrary. Answering these tough questions within the framework of existing law, consistent with our values and accounting for the legitimate needs of national security, will require a constant dialogue between lawyers, operators, and policymakers. All that we as lawyers can do is to apply in the cyber context the same rigorous approach to these hard questions that arise in the future, as we apply every day to what might be considered more traditional forms of conflict.

3. The Role of International Law in a "Smart Power" Approach to Cyberspace

This, in a nutshell, is where we are with regard to cyberconflict: We have begun work to build consensus on a number of answers, but questions continue to arise that must be answered in the months and years ahead. Beyond these questions and answers and unresolved questions, though, lies a much bigger picture, one that we are very focused on at the State Department. Which brings me to my final two questions:

Final Question 1: *Is international humanitarian law the only body of international law that applies in cyberspace?*

Final Answer 1: **No. As important as international humanitarian law is, it is *not* the only international law that applies in cyberspace.**

Obviously, cyberspace has become pervasive in our lives, not just in the national defense arena, but also through social media, publishing and broadcasting, expressions of human rights,

and expansion of international commerce, both through online markets and online commercial techniques. Many other bodies of international and national law address those activities, and how those different bodies of law overlap and interact with the laws of cyber conflict is something we will all have to work out over time.

Take human rights. At the same time that cyber activity can pose a threat, we all understand that cyber-communication is increasingly becoming a dominant mode of expression in the 21st century. More and more people express their views not by speaking on a soap box at Speakers' Corner, but by blogging, tweeting, commenting, or posting videos and commentaries. The 1948 Universal Declaration of Human Rights (UDHR) – adopted more than 70 years ago – was remarkably forward-looking in anticipating these trends. It says: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*." (emphasis added) In short, all human beings are entitled to certain rights, whether they choose to exercise them in a city square or an internet chat room. This principle is an important part of our global diplomacy, and is encapsulated in the Internet Freedom agenda about which my boss, Secretary Clinton, has spoken so passionately.

You all know of this Administration's efforts not just in the areas of cyberconflict, but also in many other cyber areas: cybersecurity, cybercommerce, fighting child pornography and other forms of cybercrime, stopping intellectual property piracy, as well as promoting free expression and human rights. So the cyberconflict issues with which this group grapples do not constitute the whole of our approach to cyberspace; they are an important part – but only a part –of this Administration's broader "smart power" approach to cyberspace.

What I have outlined today are a series of answers to cyberspace questions that the United States is on the record as supporting. I have also suggested a few of the challenging questions that remain before us, and developments over the next decade will surely produce new questions. But you should not think of these questions and answers as just a box to check before deciding whether a particular proposed operation is lawful or not. Rather, these questions and answers are part of a much broader foreign policy agenda, which transpires in a broader framework of respect for international law.

That leads to my Final Question for this group: *Why should U.S Government lawyers care about international law in cyberspace at all?*

The Answer: **Because compliance with international law *frees* us to do more, and do more legitimately, in cyberspace, in a way that more fully promotes our national interests. Compliance with international law in cyberspace is part and parcel of our broader "smart power" approach to international law as part of U.S. foreign policy.**

It is worth noting two fundamentally different philosophies about international law. One way to think about law, whether domestic or international, is as a straitjacket, a pure constraint. This approach posits that nations have serious, legitimate interests, and legal regimes restrict their ability to carry them out. One consequence of this view is that, since law is just something that constrains, it should be resisted whenever possible. Resisting so-called "extensions" of the law to new areas often seems attractive: because, after all, the old laws weren't built for these new challenges anyway, some say, so we should tackle those challenges without the legal straitjacket, while leaving the old laws behind.

But that is *not* the United States Government's view of the law, domestic or international. We see law not as a straitjacket, but as one great university calls it when it confers its diplomas, a body of "wise restraints that make us free." International law is not purely constraint, it frees us and empowers us to do things we could never do without law's legitimacy. If we succeed in

promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we *do* take will earn enhanced legitimacy worldwide for their adherence to the rule of law.

These are not new themes, but I raise them here because of they resonate squarely with the strategy we have been pursuing in cyberspace over the past few years. Of course, the United States has impressive cyber-capabilities; it should be clear from the bulk of my discussion that adherence to established principles of law does not prevent us from using those capabilities to achieve important ends. But we also know that we will be safer, the more that we can rally other States to the view that these established principles *do* impose meaningful constraints, and that there is already an existing set of laws that protect our security in cyberspace. And the more widespread the understanding that cyberspace follows established rules – and that we live by them – the stronger we can be in pushing back against those who would seek to introduce brand new rules that may be contrary to our interests.

That is why, in our diplomacy, we do not whisper about these issues. We talk *openly and bilaterally* with other countries about the application of established international law to cyberspace. We talk about these issues *multilaterally*, at the UN Group of Governmental Experts and at other fora, in promoting this vision of compliance with international law in cyberspace. We talk about them *regionally*, as when we recently co-sponsored an ASEAN Regional Forum event to focus the international community's attention on the problem of proxy actors engaging in unlawful conduct in cyberspace. Preventing proxy attacks on us is an important interest, and as part of our discussions we have outlined the ways that existing international law addresses this problem.

The diplomacy I have described is not limited to the legal issues this group of lawyers is used to facing in the operational context. These issues are interconnected with countless other cyber issues that we face daily in our foreign policy, such as cybersecurity, cyber-commerce, human rights in cyberspace, and public diplomacy through cybertools. In all of these areas, let me repeat again, *compliance with international law in cyberspace is part and parcel of our broader smart power approach to international law as part of U.S. foreign policy*. Compliance with international law – and thinking actively together about how best to promote that compliance – can only free us to do more, and to do more legitimately, in the emerging frontiers of cyberspace, in a way that more fully promotes our U.S. national interests.

Thank you very much.

Source: http://www.state.gov/s/l/releases/remarks/197924.htm, accessed 17 May 2016.

III. Department of Defense Strategy and Guidance

A. DOD Strategy for Operating in Cyberspace

The following is a fact sheet for the DOD Strategy for Operating in Cyberspace (April 2015). The full strategy can be found at: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf.

FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY

APRIL 2015

An engine of innovation and communication, the Internet connects billions of people, helps deliver goods and services globally, and brings ideas and knowledge to those who would otherwise lack access. The United States relies on the Internet and the systems and data of cyberspace for a wide range of critical services. This reliance leaves us vulnerable in the face of a real and dangerous cyber threat, as state and non-state actors plan to conduct disruptive and destructive cyberattacks on the networks of our critical infrastructure and steal U.S. intellectual property to undercut our technological and military advantage.

The purpose of the new *Department of Defense Cyber Strategy*, the Department's second, is to guide the development of DOD's cyber forces and strengthen its cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DOD's **three cyber missions: defend DOD networks, systems, and information; defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans.** The strategy sets five strategic goals and establishes specific objectives for DOD to achieve over the next five years and beyond.

What drove DOD to develop a new cyber strategy? Three major drivers required that DOD develop a new cyber strategy. First is the increasing severity and sophistication of the cyber threat to U.S. interests, to include DOD networks, information, and systems. The Department of Defense has the largest network in the world and DOD must take aggressive steps to defend its networks, secure its data, and mitigate risks to DOD missions. Second, in 2012 President Obama directed DOD to organize and plan to defend the nation against cyberattacks of significant consequence, in concert with other U.S. government agencies. This new mission required new strategic thinking. Finally, in response to the threat, in 2012 DOD began to build a Cyber Mission Force (CMF) to carry out DOD's cyber missions. The CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The strategy provides clear guidance for the CMF's development.

Building bridges to the private sector and beyond. To build the force of the future, DOD must attract the best talent, the best ideas, and the best technology to public service. To do so, DOD must build strong bridges to the private sector as well as the research institutions that make the United States such an innovative nation. The private sector and America's research institutions design and build the networks of cyberspace, provide cybersecurity services, and research and develop advanced capabilities. The Department of Defense has had a strong partnership with the private sector and these research institutions historically, and DOD will strengthen those historic ties to discover and validate new ideas for cybersecurity for DOD and for the country as a whole.

Deterrence is a key part of DOD's new cyber strategy. This strategy describes the Department of Defense contributions to a broader national set of capabilities to deter adversaries from conducting cyberattacks. The Department of Defense assumes that the deterrence of

cyberattacks on U.S. interests will be achieved through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. DOD has a number of specific roles to play in this equation; this strategy describes how DOD will fulfill its deterrence responsibilities effectively.

STRATEGIC GOALS AND KEY IMPLEMENTATION OBJECTIVES:

I. BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS. In 2013, DOD initiated a major investment in its cyber personnel and technologies for the Cyber Mission Force. The Department of Defense must train its people, build effective organizations and command and control systems, and fully develop the capabilities that DOD requires to operate in cyberspace. Key objectives of this goal include:

- Build technical capabilities for operations, to include a unified and integrated operational platform.
- Accelerate research and development to provide DOD with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace.
- Assess CMF capacity to achieve mission objectives when confronted with multiple contingencies.

II. DEFEND THE DOD INFORMATION NETWORK, SECURE DOD DATA, AND MITIGATE RISKS TO DOD MISSIONS. DOD must identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively. DOD must also plan and exercise to operate within a degraded and disrupted cyber environment in the event that an attack on DOD's networks and data succeeds, or if aspects of the critical infrastructure on which DOD relies for its operational and contingency plans are disrupted. Key objectives of this goal include:

- Build the Joint Information Environment single security architecture to shift the focus from protecting service-specific networks and systems to securing the DOD enterprise.
- Implement a capability to mitigate all known vulnerabilities that present a high risk to DOD.
- Identify, plan, and defend the networks that support key DOD missions.
- Build a layered defense around the Defense Industrial Base through improved accountability, cybersecurity standards, counterintelligence, and whole of government efforts to counter IP theft.

III. BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE. The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat cyberattacks of significant consequence on the U.S. homeland and U.S. interests. The Department of Defense must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks. Key objectives of this goal include:

- Develop intelligence and warning capabilities to anticipate threats.
- Partner with key interagency organizations to prepare to defend the nation in cyberspace.
- Work with DHS to develop continuous and automated mechanisms for sharing information.
- Assess DOD's cyber deterrence posture and provide recommendations for improving it.

IV. BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES. During heightened tensions or outright hostilities, DOD must be able to provide the President with a wide range of options for managing conflict escalation. As a part of the range of tools available to the United States, DOD must develop viable cyber options and integrate those options into Departmental plans. DOD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property.

V. BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY. All three of DOD's cyber missions require close collaboration with foreign allies and partners. In its international cyber engagement, DOD seeks to build partnership capacity in cybersecurity and cyber defense.

- Partner capacity building will focus on priority regions, to include the Middle East, Asia-Pacific, and Europe. DOD will remain adaptive and flexible to build new alliances and partnerships as required.

Source: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf, accessed 17 May 2016.

B. DOD Law of War Manual

The following is an excerpt from Chapter XVI – Cyber Operations in the *DOD Law of War Manual*, dated June 2015. The full document can be found at: http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf.

XVI – Cyber Operations

Chapter Contents

16.1 INTRODUCTION This Chapter addresses the law of war and cyber operations. It addresses how law of war principles and rules apply to relatively novel cyber capabilities and the cyber domain.

As a matter of U.S. policy, the United States has sought to work internationally to clarify how existing international law and norms, including law of war principles, apply to cyber operations.[1]

Precisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such developments.[2]

16.1. Cyberspace as a Domain. As a doctrinal matter, DOD has recognized cyberspace 16.1.1 as an n operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains.[3]

Cyberspace may be defined as "[a] global domain within the information environment consisting of interdependent networks of information technology infra structures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4]

16.1.2 Description of Cyber Operations. Cyberspace operations may be understood to be those operations that involve "[t] he employment of cyber space capabilities where the primary purpose is to achieve objectives in or through cyberspace."[5] Cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace.

16.1.2.1 *Examples of Cyber Operations*. Cyber operations include those operations that use computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Cyber operations can be a form of advance force operations, which precede the main effort in an objective area in order to prepare the objective for the main assault. For example, cyber operations may include reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code). In addition, cyber operations may be a method of acquiring foreign intelligence unrelated to specific military objectives, such as understanding technological developments or gaining information about an adversary's military capabilities and intent.

16.1.2.2 *Examples of Operations That Would Not Be Regarded as Cyber Operations.* Cyber operations generally would not include activities that merely use computers or cyberspace without a primary purpose of achieving objectives or effects in or through cyberspace. For example, operations that use computer networks to facilitate command and control, operations that use air traffic control systems, and operations to distribute information broadly using computers would generally not be considered cyber operations. Operations that target an adversary's cyberspace capabilities, but that are not achieved in or through cyberspace, would not be considered cyber operations. For example, the bombardment of a network hub, or the jamming of wireless communications, would not be considered cyber operations, even though they may achieve military objective s in cyberspace.

16.1.3 *Cyber Operations – Notes on Terminology*. DOD doctrine and terminology for cyber operations continue to develop.

16.1.3.1 *"Cyber" Versus "Cyberspace" as an Adjective*. The terms "cyber" and "cyberspace" when used as an adjective (e.g., cyber-attack, cyber defense, cyber operation) are generally used interchangeably.

16.1.3.2 *Cyber Attacks or Computer Network Attacks*. The term "attack" often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services.

Operations described as "cyber attacks" or "computer network attacks," therefore, are not necessarily "attacks" for the purposes of applying rules on conducting attacks during the conduct of hostilities.[6] Similarly, operations described as "cyber attacks" or "computer network attacks" are not necessarily "armed attacks" for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*.[7]

16.2 APPLICATION OF THE LAW OF WAR TO CYBER OPERATIONS

Specific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict.

16.2.1 Application of Specific Law of War Rules to Cyber Operations. Specific law of war rules may be applicable to cyber operations, even though these rules were developed long before cyber operations were possible.

The law of war affirmatively anticipates technological innovation and contemplates that its existing rules will apply to such innovation, including cyber operations.[8] Law of war rules may apply to new technologies because the rules often are not framed in terms of specific technological means. For example, the rules on conducting attacks do not depend on what type of weapon is used to conduct the attack. Thus, cyber operations may be subject to a variety of law of war rules depending on the rule and the nature of the cyber operation. For example, if the physical consequences of a cyber attack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyber attack would equally be subject to the same rules that apply to attacks using bombs or missiles.[9]

Cyber operations may pose challenging legal questions because of the variety of effects they can produce. For example, cyber operations could be a non-forcible means or method of conducting hostilities (such as information gathering), and would be regulated as such under rules applicable to non-forcible means and methods of warfare.[10] Other cyber operations could be used to create effects that amount to an attack and would be regulated under the rules on

conducting attacks.[11] Moreover, another set of challenging issues may arise when considering whether a particular cyber operation might be regarded as a seizure or destruction of enemy property and should be assessed as such.[12]

16.2.2 Application of Law of War Principles as a General Guide to Cyber Operations. When no specific rule applies, the principles of the law of war form the general guide for conduct during war, including conduct during cyber operations.[13] For example, under the principle of humanity, suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided in cyber operations.[14]

Certain cyber operations may not have a clear kinetic parallel in terms of their capabilities and the effects they create.[15] Such operations may have implications that are quite different from those presented by attacks using traditional weapons, and those different implications may well yield different conclusions.[16]

16.3 CYBER OPERATIONS AND *JUS AD BELLUM*

Cyber operations may present issues under the law of war governing the resort to force (i.e., *jus ad bellum*).[17]

16.3.1 Prohibition on Cyber Operations That Constitute Illegal Uses of Force Under Article 2(4) of the Charter of the United Nations. Article 2(4) of the Charter of the United Nations states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[18] Cyber operations may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law.[19] For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes.[20] Similarly, cyber operations that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under *jus ad bellum*.[21] Other factors, besides the effects of the cyber operation, may also be relevant to whether the cyber operation constitutes a use of force under *jus ad bellum*.[22]

Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibitions on the resort to force.[23]

16.3.2 Peacetime Intelligence and Counterintelligence Activities. International law and long-standing international norms are applicable to State behavior in cyberspace,[24] and the question of the legality of peacetime intelligence and counterintelligence activities must be considered on a case-by-case basis. Generally, to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law.[25] The United States conducts such activities via cyberspace, and such operations are governed by long-standing and well-established considerations, including the possibility that those operations could be interpreted as a hostile act.[26]

16.3.3 Responding to Hostile or Malicious Cyber Operations. A State's inherent right of self-defense, recognized in Article 51 of the Charter of the United Nations, may be triggered by cyber operations that amount to an armed attack or imminent threat thereof.[27] As a matter of

national policy, the United States has expressed the view that when warranted, it will respond to hostile acts in cyberspace as it would to any other threat to the country.[28]

Measures taken in the exercise of the right of national self-defense in response to an armed attack must be reported immediately to the U.N. Security Council in accordance with Article 51 of the Charter of the United Nations.[29]

16.3.3.1 *Use of Force Versus Armed Attack*. The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force.[30] Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.[31]

16.3.3.2 *No Legal Requirement for a Cyber Response to a Cyber Attack*. There is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.[32]

16.3.3.3 *Responses to Hostile or Malicious Cyber Acts That Do Not Constitute Uses of Force*. Although cyber operations that do not constitute uses of force under *jus ad bellum* would not permit injured States to use force in self-defense, those injured States may be justified in taking necessary and appropriate actions in response that do not constitute a use of force.[33] Such actions might include, for example, a diplomatic protest, an economic embargo, or other acts of retorsion.[34]

16.3.3.4 *Attribution and Self-Defense Against Cyber Operations*. Attribution may pose a difficult factual question in responding to hostile or malicious cyber operations because adversaries may be able to hide or disguise their activities or identities in cyberspace more easily than in the case of other types of operations.[35] A State's right to take necessary and proportionate action in self-defense in response to an armed attack originating through cyberspace applies whether the attack is attributed to another State or to a non-State actor.[36]

16.3.3.5 *Authorities Under U.S. Law to Respond to Hostile Cyber Acts*. Decisions about whether to invoke a State's inherent right of self-defense would be made at the national level because they involve the State's rights and responsibilities under international law. For example, in the United States, such decisions would generally be made by the President.

The Standing Rules of Engagement for U.S. forces have addressed the authority of the U.S. armed forces to take action in self-defense in response to hostile acts or hostile intent, including such acts perpetrated in or through cyberspace.[37]

16.4 CYBER OPERATIONS AND THE LAW OF NEUTRALITY

The law of neutrality may be important in certain cyber operations. For example, under the law of neutrality, belligerent States are bound to respect the sovereign rights of neutral States.[38] Because of the interconnected nature of cyberspace, cyber operations targeting networked information infrastructures in one State may create effects in another State that is not a party to the armed conflict.[39]

16.4.1 Cyber Operations That Use Communications Infrastructure in Neutral States. The law of neutrality has addressed the use of communications infrastructure in neutral States, and in certain circumstances, these rules would apply to cyber operations.

The use of communications infrastructure in neutral States may be implicated under the general rule that neutral territory may not serve as a base of operations for one belligerent against another.[40] In particular, belligerent States are prohibited from erecting on the territory of a neutral State any apparatus for the purpose of communicating with belligerent forces on land or sea, or from using any installation of this kind established by them before the armed conflict

on the territory of a neutral State for purely military purposes, and which has not been opened for the service of public messages.[41] However, merely relaying information through neutral communications infrastructure (provided that the facilities are made available impartially) generally would not constitute a violation of the law of neutrality that belligerent States would have an obligation to refrain from and that a neutral State would have an obligation to prevent.[42] This rule was developed because it was viewed as impractical for neutral States to censor or screen their publicly available communications infrastructure for belligerent traffic.[43] Thus, for example, it would not be prohibited for a belligerent State to route information through cyber infrastructure in a neutral State that is open for the service of public messages , and that neutral State would have no obligation to forbid such traffic. This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State or States).[44]

16.5 CYBER OPERATIONS AND *JUS IN BELLO*

This section addresses *jus in bello* rules and cyber operations.

16.5.1 Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks. If a cyber operation constitute s an attack, then the law of war rules on conducting attacks must be applied to those cyber operations.[45] For example, such operations must comport with the requirements of distinction and proportionality.[46]

For example, a cyber attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure, such as computer systems belonging to stock exchanges, banking systems, and universities, unless those computer systems met the test for being a military objective under the circumstances.[47] A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war.[48]

16.5.1.1 *Assessing Incidental Injury or Damage During Cyber Operations*. The proportionality rule prohibits attacks in which the expected loss of life or injury to civilians, and damage to civilian objects incidental to the attack, would be excessive in relation to the concrete and direct military advantage expected to be gained.[49]

For example, in applying the proportionality rule to cyber operations, it might be important to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but that may be networked to computers that are valid military objectives.[50]

In assessing incidental injury or damage during cyber operations, it may be important to consider that remote harms and lesser forms of harm, such as mere inconveniences or temporary losses, need not be considered in applying the proportionality rule.[51] For example, a minor, brief disruption of internet services to civilians that results incidentally from a cyber attack against a military objective generally would not need to be considered in a proportionality analysis.[52] In addition, the economic harms in the belligerent State resulting from such disruptions, such as civilian businesses in the belligerent State being unable to conduct e-commerce, generally would not need to be considered in a proportionality analysis.[53]

Even if cyber operations that constitute attacks are not expected to result in excessive incidental loss of life or injury or damage such that the operation would be prohibited by the proportionality rule, the party to the conflict nonetheless would be required to take feasible precautions to limit such loss of life or injury and damage in conducting those cyber operations.[54]

16.5.2 Cyber Operations That Do Not Amount to an "Attack" Under the Law of War. A cyber operation that does not constitute an attack is not restricted by the rules that apply to attacks.[55] Factors that would suggest that a cyber operation is not an "attack" include whether the operation causes only reversible effects or only temporary effects. Cyber operations that generally would not constitute attacks include:

- defacing a government webpage;
- a minor, brief disruption of internet services;
- briefly disrupting, disabling, or interfering with communications; and
- disseminating propaganda.

Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians or civilian objects. Nonetheless, such operations must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary.[56] Moreover, such operations should comport with the general principles of the law of war.[57]

For example, even if a cyber operation is not an "attack" or does not cause any injury or damage that would need to be considered under the proportionality rule, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons.

16.5.3 Duty to Take Feasible Precautions and Cyber Operations. Parties to a conflict must take feasible precautions to reduce the risk of incidental harm to the civilian population and other protected persons and objects.[58] Parties to the conflict that employ cyber operations should take precautions to minimize the harm of their cyber activities on civilian infrastructure and users.[59]

The obligation to take feasible precautions may be of greater relevance in cyber operations than other law of war rules because this obligation applies to a broader set of activities than those to which other law of war rules apply. For example, the obligation to take feasible precautions to reduce the risk of incidental harm would apply to a party conducting an attack even if the attack would not be prohibited by the proportionality rule.[60] In addition, the obligation to take feasible precautions applies even if a party is not conducting an attack because the obligation also applies to a party that is subject to attack.[61]

16.5.3.1 *Cyber Tools as Potential Measures to Reduce the Risk of Harm to Civilians or Civilian Objects*. In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians.[62] In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.[63]

As with other precautions, the decision of which weapon to use will be subject to many practical considerations, including effectiveness, cost, and "fragility," i.e., the possibility that once used an adversary may be able to devise defenses that will render a cyber tool ineffective in the future.[64] Thus, as with special kinetic weapons, such as precision-guided munitions that have the potential to produce less incidental damage than other kinetic weapons, cyber capabilities usually will not be the only type of weapon that is legally permitted.

16.5.4 Prohibition on Improper Use of Signs During Cyber Operations. Under the law of war, certain signs may not be used improperly.[65] These prohibitions may also be applicable during cyber operations. For example, it would not be permissible to conduct a cyber attack or to attempt to disable enemy internal communications by making use of communications that initiate non-hostile relations, such as prisoner exchanges or ceasefires.[66]

Similarly, it would be prohibited to fabricate messages from an enemy's Head of State falsely informing that State's forces that an armistice or cease-fire had been signed.[67]

On the other hand, the restriction on the use of enemy flags, insignia, and uniforms only applies to concrete visual objects; it does not restrict the use of enemy codes, passwords, and countersigns.[68] Thus, for example, it would not be prohibited to disguise network traffic as though it came from enemy computers or to use enemy codes during cyber operations.

16.5.5 Use of Civilian Personnel to Support Cyber Operations. As with non-cyber operations, the law of war does not prohibit States from using civilian personnel to support their cyber operations, including support actions that may constitute taking a direct part in hostilities.[69]

Under the GPW, persons who are not members of the armed forces, but who are authorized to accompany them, are entitled to POW status.[70] This category was intended to include, *inter alia*, civilian personnel with special skills in operating military equipment who support and participate in military operations, such as civilian members of military aircrews.[71] It would include civilian cyber specialists who have been authorized to accompany the armed forces.

Civilians who take a direct part in hostilities forfeit protection from being made the object of attack.[72]

16.6 LEGAL REVIEW OF WEAPONS THAT EMPLOY CYBER CAPABILITIES

DOD policy requires the legal review of the acquisition of weapons or weapon systems.[73] This policy would include the review of weapons that employ cyber capabilities to ensure that they are not per se prohibited by the law of war.[74] Not all cyber capabilities, however, constitute a weapon or weapons system. Military Department regulations address what cyber capabilities require legal review.[75]

The law of war does not prohibit the development of novel cyber weapons. The customary law of war prohibitions on specific types of weapons result from State practice and *opinio juris* demonstrating that a type of weapon is illegal; the mere fact that a weapon is novel or employs new technology does not mean that the weapon is illegal.[76]

Although which issues may warrant legal analysis would depend on the characteristics of the weapon being assessed, a legal review of the acquisition or procurement of a weapon that employs cyber capabilities likely would assess whether the weapon is inherently indiscriminate.[77] For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon.[78]

End Notes:

1 See, e.g. , United States Submission to the U. N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014 – 15) , 1 ("But the challenge is not whether existing international law applies to State behavior in cyberspace. As the 2012 – 13 GGE affirmed, international law does apply, and such law is essential to regulating State conduct in this domain. The challenge is providing decision-makers with considerations that may be taken into account when determining how existing international law applies to cyber activities. Despite this challenge, history has shown that States, through consultation and cooperation, have repeatedly and successfully applied existing bodies of law to new technologies. It continues to be the U.S. view that all States will benefit from a stable international ICT [information and communication technologies] environment in which existing international law is the foundation for responsible State behavior in cyberspace."); Barack Obama, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World , 9 (May 2011) ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior — in times of peace and conflict — also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how

these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace."); DEPARTMENT OF DEFENSE , Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 , 7 - 8 (Nov. 2011) ("The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas.").

2 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 464 - 65 (2002) ("The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations. ... Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.").

3 William J. Lynn III, Deputy Secretary of Defense, Defending a New Domain: The Pentagon's Cyberstrategy, 89 FOREIGN AFFAIRS 97, 101 (Sept./Oct. 2010) ("As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it.").

4 JOINT PUBLICATION 3-12, Cyberspace Operations, GL-4 (Feb. 5, 2013) ("(U) Cyberspace. A global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.").

5 JOINT PUBLICATION 3-0, Joint Operations (Aug. 11, 2011) ("cyberspace operations. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.").

6 Refer to § 16.5.1 (Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks).

7 Refer to § 16.3.3 (Responding to Hostile or Malicious Cyber Operations).

8 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 3 (Dec. 2012) ("Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint. Think of it this way. This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law — international humanitarian law, or the law of armed conflict — affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation.").

9 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) , reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE , 3 - 4 (Dec. 2012) ("In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. ... Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.").

10 Refer to § 5.26 (Non-Forcible Means and Methods of Warfare). 11 Refer to § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

12 Refer to § 5.17 (Seizure and Destruction of Enemy Property).

13 Refer to § 2.1.2.2 (Law of War Principles as a General Guide).

14 Refer to § 2.3 (Humanity).

15 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) , reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE , 7 (Dec. 2012) ("I have also noted some clear-cut cases where the physical effects of a hostile cyber action would be comparable to what a kinetic action could achieve: for example, a bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result. As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'").

16 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 490 (2002) ("In the process of reasoning by analogy to the law applicable to traditional weapons, it must always be kept in mind that computer network attacks are likely to present implications that are quite different from the implications presented by attacks with traditional weapons. These different implications may well yield different conclusions.").

17 Refer to § 1.11 (*Jus ad Bellum*).

18 U.N. C HARTER art. 2(4).

19 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) reprinted in 54 H ARVARD I NTERNATIONAL LAW JOURNAL ONLINE, 3 (Dec. 2012) ("Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.").

20 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) , reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE , 4 (Dec. 2012) ("Commonly cited examples of cyber activity that would constitute a use of force include, for example, (1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.").

21 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 483 (2002) ("Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.").

22 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) , reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE , 4 (Dec. 2012) ("In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.").

23 Refer to § 1.11.3 (Prohibition on Certain Uses of Force).

24 Refer to § 16.1 (Introduction).

25 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 518 (2002).

26 DEPARTMENT OF DEFENSE, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 6 - 7 (Nov. 2011).

27 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 4 (Dec. 2012) ("Question 4: May a state ever respond to a computer network attack by exercising a right of national self-defense? Answer 4: Yes. A state's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."); Barack Obama, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 1 0 (May 2011) ("Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace.").

28 Barack Obama, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 14 (May 2011) ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means — diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.").

29 Refer to § 1.11.5.6 (Reporting to the U.N. Security Council).

30 Refer to § 1.11.5.2 (Use of Force Versus Armed Attack).

31 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), reprinted in 54 H ARVARD I NTERNATIONAL L AW JOURNAL ONLINE, 7 (Dec. 2012) ("To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response — such responses must still be necessary and of course proportionate.").

32 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) reprinted in 54 H ARVARD I NTERNATIONAL LAW JOURNAL

ONLINE, 4 (Dec. 2012) ("There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.").

33 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 482 (2002) ("There is also a general recognition of the right of a nation whose rights under international law have been violated to take countermeasures against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force. For example, an arbitral tribunal in 1978 ruled that the United States was entitled to suspend French commercial air flights into Los Angeles after the French had suspended U.S. commercial air flights into Paris. Discussions of the doctrine of countermeasures generally distinguish between countermeasures that would otherwise be violations of treaty obligations or of general principles of international law (in effect, reprisals not involving the use of armed force) and retorsions – actions that may be unfriendly or even damaging, but which do not violate any international legal obligation. The use of countermeasures is subject to the same requirements of necessity and proportionality as apply to self-defense.").

34 Refer to § 18.17 (Retorsion).

35 DEPARTMENT OF DEFENSE , Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 , 4 (Nov. 2011) ("The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage. The Department recognizes that deterring malicious actors from conducting cyber attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors.").

36 United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013, 2 ("As the United States noted in its 2010 submission to the GGE, the following established principles would apply in the context of an armed attack, whether it originated through cyberspace or not: • The right of self-defense against an imminent or actual armed attack applies whether the attacker is a State actor or a non-State actor"). Refer to § 1.11.5.4 (Right of Self-Defense Against Non-State Actors).

37 See, e.g., CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces, 6b(1) (June 13, 2005), reprinted in INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, U.S. ARMY, OPERATIONAL LAW HANDBOOK 95 (2007) ("Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unless otherwise directed by a unit commander as detailed below, military members may exercise individual self-defense in response to a hostile act or demonstrated hostile intent.").

38 Refer to § 15.3.1 (Neutral Rights).

39 Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 6 (Dec. 2012) ("States conducting activities in cyberspace must take into account the sovereignty of other states, including outside the context of armed conflict. The physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial state. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered.").

40 Refer to § 15.5 (Prohibition on the Use of Neutral Territory as a Base of Operations).

41 Refer to § 15.5.3 (Prohibition Against Establishment or Use of Belligerent Communications Facilities in Neutral Territory).

42 Refer to § 15.5.3.1 (Use of Neutral Facilities by Belligerents Not Prohibited).

43 Colonel Borel, Report to the Conference from the Second Commission on Rights and Duties of Neutral States on Land, in JAMES BROWN SCOTT, THE REPORTS TO THE HAGUE CONFERENCES OF 1899 AND 1907, 543 (1917) ("We are here dealing with cables or apparatus belonging either to a neutral State or to a company or individuals, the operation of which, for the transmission of news, has the character of a public service. There is no reason to compel the neutral State to restrict or prohibit the use by the belligerents of these means of communication. Were it otherwise, objections of a practical kind would be encountered, arising out of the considerable difficulties in exercising control, not to mention the confidential character of telegraphic correspondence and the rapidity necessary to this service. Through his Excellency Lord Reay, the British delegation requested that it be specified that 'the liberty of a neutral State to transmit messages, by means of its telegraph lines on land, its submarine cables or its wireless apparatus, does not imply that it has any right to use them or permit their use in order to render manifest assistance to one of the belligerents'. The justice of the idea thus stated was so great as to receive the unanimous approval of the Commission.").

44 See DEPARTMENT OF DEFENSE, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 8 (Nov. 2011) ("The issue of the legality of transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight rights.' There is currently no international consensus regarding the definition of a 'cyber weapon.' The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult. Most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action."); Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 489 (2002) ("There need be less concern for the reaction of nations through whose territory or communications systems a destructive message may be routed. If only the nation's public communications systems are involved, the transited nation

will normally not be aware of the routing such a message has taken. Even if it becomes aware of the transit of such a message and attributes it to the United States, there would be no established principle of international law that it could point to as being violated. As discussed above, even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft.").

45 Refer to § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

46 Refer to § 5.6 (Discrimination in Conducting Attacks); § 5.12 (Proportionality in Conducting Attacks).

47 Refer to § 5.7 (Military Objectives).

48 Refer to § 5.17.2 (Enemy Property – Military Necessity Standard).

49 Refer to § 5.12 (Proportionality in Conducting Attacks).

50 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 8 (Dec. 2012) ("As you all know, information and communications infrastructure is often shared between state militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack, including in the cyber realm. But how, exactly, are the *jus in bello* rules to be implemented in cyberspace? Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review. Any number of factual scenarios could arise, however, which will require a careful, fact-intensive legal analysis in each situation.").

51 Refer to § 5.12.2 (Types of Harm – Loss of Life, Injury, and Damage).

52 Cf. Program on Humanitarian Policy and Conflict Research at Harvard University, Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare, 28 (A.1.e.7) (2010) ("The definition of 'attacks' also covers 'non-kinetic' attacks (i.e. attacks that do not involve the physical transfer of energy, such as certain CNAs [computer network attacks]; see Rule 1(m)) that result in death, injury, damage or destruction of persons or objects. Admittedly, whether 'non-kinetic' operations rise to the level of an 'attack' in the context of the law of international armed conflict is a controversial issue. There was agreement among the Group of Experts that the term 'attack' does not encompass CNAs that result in an inconvenience (such as temporary denial of internet access).").

53 Refer to § 5.12.2 (Types of Harm – Loss of Life, Injury, and Damage).

54 Refer to § 16.5.3 (Duty to Take Feasible Precautions and Cyber Operations).

55 Refer to § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

56 Refer to § 5.3.2.1 (Non-Violent Measures That Are Militarily Necessary).

57 Refer to § 16.2.2 (Application of Law of War Principles as a General Guide to Cyber Operations).

58 Refer to § 5.3.3 (Affirmative Duties to Take Feasible Precautions for the Protection of Civilians and Other Protected Persons and Objects).

59 United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013, 4 ("The law of war also requires warring States to take all practicable precautions, taking into account military and humanitarian considerations, to avoid and minimize incidental death, injury, and damage to civilians and civilian objects. In the context of hostilities involving information technologies in armed conflict, parties to the conflict should take precautions to minimize the harm of such cyber activities on civilian infrastructure and users.").

60 Refer to § 5.11 (Feasible Precautions in Conducting Attacks to Reduce the Risk of Harm to Protected Persons and Objects).

61 Refer to § 5.14 (Feasible Precautions to Reduce the Risk of Harm to Protected Persons and Objects by the Party Subject to Attack).

62 Refer to § 5.11.3 (Selecting Weapons (Weaponeering)).

63 United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013 , 4 ("Cyber operations that result in non-kinetic or reversible effects can be an important tool in creating options that minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.").

64 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 490 (2002) ("Another possible implication of a defender's technological prowess may arise when a nation has the capacity for graduated self-defense measures. Some may argue that a nation having such capabilities must select a response that will do minimal damage. This is a variant of the argument that a nation possessing precision-guided munitions must always use them whenever there is a potential for collateral damage. That position has garnered little support among nations and has been strongly rejected by the United States. There is broad recognition that the risk of collateral damage is only one of many military considerations that must be balanced by

military authorities planning an attack. One obvious consideration is that a military force that goes into a protracted conflict with a policy of always using precision-guided munitions whenever there is any potential for collateral damage will soon exhaust its supply of such munitions. Similarly, military authorities must be able to weigh all relevant military considerations in choosing a response in self-defense against computer network attacks. These considerations will include the probable effectiveness of the means at their disposal, the ability to assess their effects, and the "fragility" of electronic means of attack (i.e., once they are used, an adversary may be able to devise defenses that will render them ineffective in the future).").

65 Refer to § 5.24 (Improper Use of Certain Signs).

66 Refer to § 12.2 (Principle of Good Faith in Non-Hostile Relations).

67 Department of Defense, Office of the General Counsel, An Assessment of International Legal Issues in Information Operations (2nd ed., Nov. 1999), reprinted in 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 473 (2002) ("Perfidy: It may seem attractive for a combatant vessel or aircraft to avoid being attacked by broadcasting the agreed identification signals for a medical vessel or aircraft, but such actions would be a war crime. Similarly, it might be possible to use computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this would also be a war crime.").

68 Refer to § 5.23.1.5 (Use of Enemy Codes, Passwords, and Countersigns Not Restricted).

69 Refer to § 4.15.2 .2 (Employment in Hostilities).

70 Refer to § 4.15 (Persons Authorized to Accompany the Armed Forces).

71 Refer to § 4.15 (Persons Authorized to Accompany the Armed Forces).

72 Refer to § 5.9 (Civilians Taking a Direct Part in Hostilities).

73 Refer to § 6.2 (DOD Policy of Reviewing the Legality of Weapons).

74 Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) , reprinted in 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE , 6 (Dec. 2012) ("States should undertake a legal review of weapons, including t hose that employ a cyber capability. Such a review should entail an analysis, for example, of whether a particular capability would be inherently indiscriminate, i.e., that it could not be used consistent with the principles of distinction and proportionality. The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict: first, an evaluation of new weapons to determine whether their use would be per se prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.").

75 See, e.g., DEPARTMENT OF THE ARMY REGULATION 27-53, Review of Legality of Weapons Under International Law (Jan. 1, 1979); SECRETARY OF THE N AVY INSTRUCTION 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System (Sept. 1, 2011); DEPARTMENT OF THE AIR FORCE INSTRUCTION 51-402, Legal Reviews of Weapons and Cyber Capabilities (Jul. 27, 2011).

76 Refer to § 6.2.1 (Review of New Types of Weapons).

77 Refer to § 6.7 (Inherently Indiscriminate Weapons).

78 United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013, 3 ("Weapons that cannot be directed at a specific military objective or whose effects cannot be controlled would be inherently indiscriminate, and per se unlawful under the law of armed conflict. In the traditional kinetic context, such inherently indiscriminate and unlawful weapons include, for example, biological weapons. Certain cyber tools could, in light of the interconnected nature of the network, be inherently indiscriminate in the sense that their effects cannot be predicted or controlled; a destructive virus that could spread uncontrollably within civilian internet systems might fall into this category. Attacks using such tools would be prohibited by the law of war.").

Source: www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf, accessed 17 May 2016.

IV. Joint and Service Doctrine

A. Joint Cyberspace Operations Doctrine

Joint Cyberspace Operations doctrine is set down in Joint Publication 3-12 (R) dated 5 Feb 2013. This section extracts the publication's executive summary. The full document can be found at: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Introduces cyberspace and its integration into joint operations.**
- **Explains cyberspace operations and their relationship to joint functions.**
- **Covers authorities, roles, and responsibilities.**

Introduction

Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Most aspects of joint operations rely in part on cyberspace, the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Developments in cyberspace provide the means for the U.S. military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the operational environment (OE), and can be leveraged to ensure the nation's economic and physical security. Access to the Internet provides adversaries the capability to compromise the integrity of U.S. critical infrastructures in direct and indirect ways. These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the U.S. in general and the joint force in particular.

Cyberspace

Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space.

Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. The **physical network** layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The **logical network** layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. The **cyber-persona** layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital

representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.

Integrating CO

While it is possible that some military objectives can be achieved by CO alone, CO capabilities should be considered during joint operation planning, integrated into the joint force commander's plan, and synchronized with other operations during execution.

Commanders conduct cyberspace operations (CO) to retain freedom of maneuver in cyberspace, accomplish the joint force commander's (JFC's) objectives, deny freedom of action to adversaries, and enable other operational activities. Conflicts that may need to be addressed to fully integrate CO into joint operation planning and execution include: centralized CO planning for Department of Defense information network (DODIN) operations and defense; the JFC's need to synchronize operations and fires, including CO; deconfliction requirements between government entities; partner nation relationships; and the relationships between CO and information operations, between CO and operations conducted in the physical domains, and the wide variety of legal issues that relate to CO.

The Joint Force and Cyberspace

The JFC faces a unique set of challenges while executing CO in a complex global security environment. CO are enabled by the DODIN. The DODIN is a global infrastructure of Department of Defense (DOD) systems carrying DOD, national security, and related intelligence community information and intelligence. Cyberspace presents the JFC with many threats ranging from nation states to individual actors. Perhaps the most challenging aspect of attributing actions in cyberspace is connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor, with sufficient confidence and verifiability to hold them accountable. CO may not require physical proximity; many CO can be executed remotely. Moreover, the effects of CO may extend beyond a target, a joint operations area, or even an area of responsibility (AOR).

JP 3-12(R) contains four chapters:

Chapter I. Introduction

Chapter II. Cyberspace Operations

Chapter III. Authorities, Roles and Responsibilities

Chapter IV. Planning and Coordination

Appendix A. References

Appendix B. Administrative Instructions

Source: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, accessed 17 May 2016.

B. Army Cyber Electromagnetic Activities Doctrine

Army Cyber Electromagnetic Activities doctrine is set down in Field Manual 3-38 dated February 2014. This section extracts the publication's Introduction section. The full document can be found at: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

Introduction

U.S. forces operate in an increasingly network-based world. The proliferation of information technologies is changing the way humans interact with each other and their environment, including interactions during military operations. This broad and rapidly changing operational environment requires that today's Army must operate in cyberspace and leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested.

FM 3-38, *Cyber Electromagnetic Activities* (CEMA) is the first doctrinal field manual of its kind. The integration and synchronization of CEMA is a new concept. The Army codified the concept of CEMA in Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*, and ADP 6-0, *Mission Command*. The purpose of FM 3-38 is to provide an overview of principles, tactics, and procedures on Army integration of CEMA as part of unified land operations.

At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum (EMS) and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO).

The Army continues to support the SecDef and joint requirements for information operations, EW, and cyberspace operations through the execution of CEMA and the integration of other information-related activities. These separate activities are tied through mission command, but they have distinctly different processes for carrying out their operating requirements.

FM 3-38 contains seven chapters:

Chapter 1 defines CEMA and provides an understanding of the fundamentals of the CEMA staff tasks. It briefly describes each activity and provides a framework for the emerging operational environment that includes cyberspace.

Chapter 2 begins with a discussion of the commander's role in the conduct of CEMA. It then describes the CEMA element, its role in the operations process, and how it interacts with, supports, and receives support from other staff members.

Chapter 3 provides tactics and procedures specific to cyberspace operations.

Chapter 4 provides tactics and procedures specific to EW.

Chapter 5 provides tactics and procedures specific to SMO and the functions executed by the spectrum manager.

Chapter 6 describes how CEMA are executed through the operations processes, including other integrating processes.

Chapter 7 describes considerations unique to CEMA when conducting operations with unified action partners.

Appendix A provides guidance on CEMA input to operations orders and plans

Source: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf, accessed on 17 May 2016.

C. Marine Corps Cyberspace Operations Doctrine

MCIP 3-40.02, *Marine Corps Cyberspace Operations*, dated 6 October 2014, is not available to the public. The following is an excerpt of the Cyberspace Operations section from MCDP 1-0, *Marine Corps Operations*. The full document can be found at: http://www.marines.mil/Portals/59/Publications/MCDP%201-0%20Marine%20Corps%20Operations.pdf.

Cyberspace Operations

Cyberspace may be described as a global domain that leverages information and telecommunication technologies to create an environment of interdependent computer and telecommunication networks, including command and control systems, which can be used to produce outcomes in virtual and physical realms.

The ability to operate in cyberspace is critical to strategic, operational, and tactical successes. Without secure computerized technologies, many weapon and command and control systems will not function properly; intelligence, surveillance, and reconnaissance systems will be ineffective; and sensitive information will be at risk of compromise. The Marine Corps and other Services depend on cyberspace operations for speed, precision, and lethality. Adversaries recognize that much of the United States' economic and military dominance relies upon the technology, communications, and automated systems that cyberspace enables. Ease of access and rate of technological change combine to make dominance in this domain tenuous and invite asymmetric challenges. Challenges range from recreational hackers to self-styled cyber-vigilantes, groups with nationalistic or ideological agendas, terrorist organizations, transnational actors, international corporations with ties to other governments, and nation states.

Cyberspace operations involve the employment of cyber capabilities where the primary purpose is to create military objectives or effects in or through cyberspace. Cyberspace operations comp rise five broad categories—Department of Defense network operations, defensive cyber operations, offensive cyber operations, computer network exploitation, and information assurance.

- Network operations are Department of Defense-wide operational, organizational, and technical capabilities employed to operate and defend the Department of Defense information network. This network is the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, managing, and disseminating information on demand to warfighters, policy makers, and support personnel. Marine Corps network operations include day-to-day operations required to maintain the Marine Corps Enterprise Network and protect it from both external and internal threats.
- Defensive cyber operations involves actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information network. Defensive cyber operations employs information technology, information assurance, intelligence, counterintelligence, law enforcement, and other military capabilities to defend Department of Defense information network.
- Offensive cyber operations includes the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, within the computers and networks themselves, or to enable future offensive operations.
- Computer network attack is a subset of offensive cyberspace operations where the anticipated effect of the operation is equivalent to a military attack.

- Computer network exploitation is intelligence collection activities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
- Information assurance includes measures that protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Given the scope and complexity of cyberspace operations, they must be carefully integrated into the overall joint and Marine Corps operational planning and effectively coordinated to achieve designated operational and tactical objectives.

Source: http://www.marines.mil/Portals/59/Publications/MCDP%201-0%20Marine%20Corps%20Operations.pdf, accessed on 17 May 2016.

D. Navy Cyberspace Operations Doctrine and Strategic Plan

NWP 3-12, *Cyberspace Operations* is classified. The following is an excerpt of the Executive Summary of *Navy Cyber Power 2020*, dated November 2012. This Strategic Plan provides the framework and vision necessary to ensure the U.S. Navy remains a critical insurer of our national security and economic prosperity well into the future. The full document can be found at: http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf.

Executive Summary

U.S. maritime power is comprised of six core capabilities: forward presence, deterrence, sea control, power projection, maritime security, and humanitarian assistance/disaster response (HA/DR). In today's highly networked world each one of these core capabilities is enhanced by effective Navy cyberspace operations.

Navy Cyber Power 2020 (NCP 2020) is a strategy for achieving the Navy's vision for cyberspace operations (Figure 1). This document describes the key end-state characteristics that the Navy must create and the major strategic initiatives we will pursue to achieve success. It serves as a guidepost to inform our enterprise architecture, investment decisions, and future roadmaps.

U.S. Fleet Cyber Command led an assessment of cyber threats, key trends, and challenges impacting Navy cyberspace operations to identify critical opportunities that will enable the Navy to maintain its advantages in cyberspace. To achieve the Navy's vision for cyberspace operations the Navy will address cyber threats, key trends, and challenges by pursuing several strategic initiatives across four key focus areas: Integrated Operations, Optimized Cyber Workforce, Technology Innovation, and Requirements, PPBE & Acquisition Reform.

The Navy will pursue every opportunity to execute NCP 2020 strategic initiatives in conjunction with industry, academia, interagency, Service, Joint, and Allied partners to maximize integration and ensure the most efficient use of defense resources. The Navy will also institute a set of strategic performance measures for each key focus area to evaluate progress and ensure that we are achieving the desired effect.

NCP 2020 sets out an ambitious agenda. The strategic initiatives described in this document are critical to ensuring our operational advantage in the maritime domain. Collectively these efforts represent a fundamental change in the way we conduct operations and manage the Navy. Success requires an "all hands" effort, from the Pentagon to the deck plate.

Navy cyberspace operations provide Navy and Joint commanders with an operational advantage by:

- Assuring access to cyberspace and confident Command and Control
- Preventing strategic surprise in cyberspace
- Delivering cyber effects

Source: http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf, accessed 17 May 2016.

E. Air Force Cyberspace Operations Doctrine

Air Force Cyberspace Operations doctrine is set down in Annex 3-12 last updated 20 November 2011. This section extracts the publication's Table of Contents and Introduction sections. The full document can be found at: https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf.

Catalog of Doctrine Topics

Introduction to Cyberspace Operations

Cyberspace superiority may be localized in time and space, or it may be broad and enduring. The concept of cyberspace superiority hinges on the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects. "Supremacy" prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations. While "supremacy" is most desirable, it may not be operationally feasible. Cyberspace superiority, even local or mission-specific cyberspace superiority, may provide sufficient freedom of action to create desired effects. Therefore, commanders should determine the minimum level of control required to accomplish their mission and assign the appropriate level of effort.

https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf, accessed 17 May 2016.

This Page Intentionally Blank

Appendix B: U.S. Cyberspace Organizations

Appendix B includes:

I. **Department of State**
   - **Office of the Coordinator for Cyber Issues**

II. **Department of Homeland Security**
   - **Office of Cybersecurity and Communications**

II. **Depart of Defense**
   - **National Security Agency (NSA)**
   - **Department of Defense Chief Information Officer (DOD CIO)**
   - **Defense Information Systems Agency (DISA)**

III. **Joint Organizations**
   - **Joint Staff, Deputy Director for Global Operations (DDGO)**
   - **Joint Spectrum Center (JSC)**
   - **Joint Communications Support Element (JCSE)**
   - **U.S. Cyber Command (USCYBERCOM)**

IV. **Service Organizations**
   - **Army Cyber Command (ARCYBER) / 2nd Army**
   - **Network Enterprise Technology Command (NETCOM)**
   - **Intelligence and Security Command (INSCOM)**
   - **1st Information Operations Command (Land)**
   - **Army Chief Information Officer/G-6 (CIO/G-6)**
   - **Marine Corps Forces Cyber (MARFORCYBER)**
   - **Navy U.S. Fleet Cyber / U.S. TENTH Fleet (FCC-C10F)**
   - **Air Forces Cyber / 24th Air Force**

I. Department of State - Office of the Coordinator for Cyber Issues

1. In partnership with other countries, the State Department is leading the U.S. Government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.

2. To more effectively advance the full range of U.S. interests in cyberspace, as outlined in the U.S. International Strategy for Cyberspace, the Office of the Coordinator for Cyber Issues (S/CCI) was established in February 2011.

3. S/CCI brings together the many elements in the State Department working on cyber issues. Its responsibilities include:

- Coordinating the Department's global diplomatic engagement on cyber issues
- Serving as the Department's liaison to the White House and federal departments and agencies on these issues
- Advising the Secretary and Deputy Secretaries on cyber issues and engagements
- Acting as liaison to public and private sector entities on cyber issues
- Coordinating the work of regional and functional bureaus within the Department engaged in these areas

4. S/CCI's coordination function spans the full spectrum of cyber-related issues to include security, economic issues, freedom of expression, and free flow of information on the Internet.

5. The S/CCI provides a series of information papers on cyberspace related topics on its webpage. These documents include excerpts from the Secretary of State's speech in the Republic of Korea on 18 May 2015:

- *"The basic rules of international law apply in cyberspace. We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace. First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure. Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm. Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain. Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way. And fifth, every country should do what it can to help states that are victimized by a cyberattack.* [123]
- "The United States is also working with partners to improve network defenses and in cooperation with other countries to respond to cyber incidents. All of this is crucial, because in an interconnected system like the Internet, poor cybersecurity has the potential to increase the danger for all of us. So we have to help each other. We have to maintain direct contact between our incident response teams, invest heavily in that capacity, and build that capacity so that weak spots are turned into stronger blockages against the vulnerabilities, and ultimately, they disappear."[124]

Source: http://www.state.gov/s/cyberissues/, accessed 17 May 2016.

II. Department of Homeland Security - Office of Cybersecurity and Communications (CS&C)

The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. CS&C leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.

As the Sector-Specific Agency for the Communications and Information Technology (IT) sectors, CS&C coordinates national-level reporting that is consistent with the National Response Framework (NRF).

Structure: Congress created the Office of the Assistant Secretary for Cybersecurity and Communications in 2006. CS&C carries out its mission through its five divisions:

The Office of Emergency Communications (OEC): The OEC supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. The office leads the Nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. OEC provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide.

The National Cybersecurity and Communications Integration Center (NCCIC): Information sharing is a key part of the Department of Homeland Security's (DHS) mission to create shared situational awareness of malicious cyber activity. Cyberspace has united once distinct information structures, including our business and government operations, our emergency preparedness communications, and our critical digital and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of the nation's critical infrastructure and key resources; therefore, to our economic and national security. DHS's NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.

Stakeholder Engagement and Cyber Infrastructure Resilience: The Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division is the Department of Homeland Security (DHS) primary point of engagement and coordination for national security/emergency preparedness (NS/EP) communications and cybersecurity initiatives for both government and industry partners, and is the Executive Secretariat for the Joint Program Office for the NS/EP Communications Executive Committee. CS&C relies on SECIR to streamline coordination and engagement with external partners, while

leveraging capabilities and significant subject matter expertise in order to meet stakeholder requirements.

Federal Network Resilience (FNR): The FNR division is responsible for developing innovative approaches to drive change in cybersecurity risk management by focusing on establishing metrics that have measureable impact on improving cybersecurity for Federal Civilian Executive Branch departments and agencies; gathering cybersecurity requirements and developing operational policies for the federal government; collaborating with, and providing outreach to, the Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council, and individual agency Chief Information (CIOs) and Chief Information Security Officers (CISOs); and leveraging best practices across CS&C and lessons learned in support of Federal Civilian Executive Branch departments' and agencies' cyber hygiene.

Network Security Deployment (NSD): The NSD division serves as the cybersecurity engineering and acquisition "Center of Excellence" within CS&C. In support of that role, NSD provides development, acquisition, deployment, operational, and customer support to satisfy the Department's mission requirements under the Comprehensive National Cybersecurity Initiative (CNCI).

In addition, CS&C operates the Enterprise Performance Management Office, which ensures that the Assistant Secretary's strategic goals and priorities are reflected across all CS&C programs; measures the effectiveness of initiatives, programs, and projects that support those goals and priorities; and facilitates cross-functional mission coordination and implementation between CS&C components, within DHS, and among the interagency.

Source: https://www.dhs.gov/office-cybersecurity-and-communications, accessed 17 May 2016.

III. Department of Defense

A. National Security Agency/Central Security Service (NSA/CSS)

Mission. The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.

The **Central Security Service (CSS)** provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community. It promotes full partnership between the NSA and the cryptologic elements of the Armed Forces, and teams with senior military and civilian leaders to address and act on critical military-related issues in support of national and tactical intelligence objectives. CSS coordinates and develops policy and guidance on the Signals Intelligence and Information Assurance missions of NSA/CSS to ensure military integration.

- The CSS was established by presidential directive in 1972 to promote full partnership between NSA and the Service Cryptologic Components of the U.S. Armed Forces. This new command created a more unified cryptologic effort by combining NSA and CSS. The Director of NSA is dual-hatted as the Chief of CSS.

The **Information Assurance (IA)** mission at the National Security Agency (NSA) serves a role unlike that of any other U.S. Government entity. National Security Directive (NSD) 42 authorizes NSA to secure National Security Systems, which includes systems that handle classified information or are otherwise critical to military or intelligence activities. IA has a pivotal leadership role in performing this responsibility, and partners with government, industry, and academia to execute the IA mission.

- Now that cyberspace is the primary arena in which we protect information, we are working toward shaping an agile and secure operational cyber environment where we can successfully outmaneuver any adversary. A key step in building Confidence in Cyberspace is a willingness to offer what we know.

Signals Intelligence (SIGINT). The National Security Agency is responsible for providing foreign SIGINT to our nation's policy-makers and military forces. SIGINT plays a vital role in our national security by providing America's leaders with critical information they need to defend our country, save lives, and advance U.S. goals and alliances globally.

- SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.
- NSA's SIGINT mission is specifically limited to gathering information about international terrorists and foreign powers, organizations, or persons. NSA produces intelligence in response to formal requirements levied by those who have an official need for intelligence, including all departments of the Executive Branch of the United States Government.

Cyber. NSA's SIGINT and Information Assurance missions come together to detect and prevent threats to official U.S. government networks. SIGINT and IA analysts work together around the clock to assess foreign threats to networks. They also enable the U.S. military and our allies to carry out integrated computer network operations.

Support to the Military. The National Security Agency is part of the U.S. Department of Defense, serving as a combat support agency. Supporting our military service members around the world is one of the most important things that we do.

- We provide intelligence support to military operations through our signals intelligence activities, while our information assurance personnel, products and services ensure that military communications and data remain secure, and out of the hands of our adversaries.
- We provide wireless and wired secure communications to our warfighters and others in uniform no matter where they are, whether traveling through Afghanistan in a Humvee, diving beneath the sea, or flying into outer space. Our information assurance mission also produces and packages the codes that secure our nation's weapons systems.
- Additionally, we set common protocols and standards so that our military can securely share information with our allies, NATO and coalition forces around the world. Interoperability is a key to successful joint operations and exercises.
- To support our military customers, NSA has deployed personnel to all of the major military commands and to locations around the globe where there is a U.S. military presence. NSA analysts, linguists, engineers and other personnel deploy to Afghanistan and other hostile areas to provide actionable SIGINT and information assurance support to warfighters on the front lines. Many of our deployed personnel serve in Cryptologic Services Groups, providing dedicated support at the Combatant Command or headquarters level. Since the mid-2000s, however, NSA personnel have also been serving on Cryptologic Support Teams, which are assigned to support smaller units such as Brigade Combat Teams to ensure they are receiving the intelligence and information assurance products and services they need to accomplish their specific missions. These teams have enabled NSA to push the full capabilities of our global cryptologic enterprise as far forward as possible.

Customers & Partners. Many agencies and services rely on NSA's expertise in foreign signals intelligence and information assurance for mission success. NSA supports the highest levels of government such as the Office of the President all the way down to the warfighter deployed overseas in a combat zone. In addition, NSA knows that the job protecting America's security is important to accomplish alone. NSA has many partners, both inside the United States and with foreign governments.

Source: https://www.nsa.gov/about/, accessed 17 May 2016.

B. Department of Defense Chief Information Officer (DOD CIO)

About DOD CIO: As the Principal Staff Assistant and senior Information Technology advisor to the Secretary of Defense, the Department of Defense Chief Information Officer is responsible for all matters relating to the Department's information enterprise.

DOD is huge. It has over 1.4 million active-duty men and women, 718,000 civilians, and 1.1 million National Guard and Reserve members. More than 450,000 of its employees are overseas. It also has several hundred thousand buildings and structures located in more than 5,000 different locations or sites, as well as more than seven million computers and IT devices.

And DOD is very mobile. This means that DOD picks up big chunks of its organization and networks, then puts them down in different places around the world. This type of mobility is required to help DOD defeat ISIL, train partner nations, accomplish humanitarian missions, and provide disaster relief.

The Department also regularly undertakes these missions with partners, some expected, some unexpected. So not only do DOD's networks need to be mobile, but they need to be flexible – and secure enough for the mission. Finally, the Department's IT is complicated – DOD is in almost every business you can imagine, like acquisitions, health, logistics, real estate, food distribution, and more.

Mission: The DOD CIO is the Principal Staff Assistant and senior Information Technology advisor to the Secretary of Defense. This role includes overseeing many national security and defense business systems, managing information resources, and finding efficiencies. It is responsible for all matters relating to the Department's information enterprise, including:

- Communications
- Spectrum management
- Network policy and standards
- Information systems
- Cybersecurity
- Positioning, navigation, and timing policy
- DOD information enterprise that supports DOD command and control

Top Priorities: DOD CIO is ensuring a more secure, efficient, effective DOD IT environment through its top priorities:

- Modernizing the networks – fielding the Joint Regional Security Stacks is the CIO's top priority
- Sharing with mission partners by establishing the Mission Partner Environment
- Reducing the cost of DOD IT through a review directed by the Deputy SecDef
- Managing DOD's data by partnering with industry to migrate data to the cloud
- Defending against cyber attack is the CIO's highest cyber priority
- Empowering mobile data access through people and information across the Department
- Maximize Spectrum Access to Enhance Operational Effectiveness in an increasingly congested and contested environment

Source: http://dodcio.defense.gov/, accessed 17 May 2016.

C. Defense Information Systems Agency (DISA)

Vision: Information superiority in defense of our Nation.

Mission: DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations.

The Objective State: Provide assured, scalable, managed access to services and data at the point of need and in all environments through cost-effective infrastructure and computing.

Our Work/DISA 101: DISA is a combat support agency of the Department of Defense (DOD). The agency is composed of nearly 6,000 civilian employees; more than 1,500 active duty military personnel from the Army, Air Force, Navy, and Marine Corps; and approximately 7,500 defense contractors. The agency provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations.

DISA's Mission Partners: The Mission Partner Engagement Office and Engagement Executives are DISA's principal representatives for receiving Mission Partner (MP) requests, DISA outreach to MPs, advocating for MP issues, and providing a conduit for MP feedback to DISA.

Chain of Command: DISA reports to the DOD Chief Information Officer (CIO). The Office of the DOD CIO is the department's primary authority for the policy and oversight of information resources management, to include matters related to information technology (IT), network defense, and network operations. The DOD CIO exercises authority, direction, and control over the director of DISA and organizationally reports to the SecDef.

As information technology (IT) combat support agency, DISA is committed to providing enterprise-level IT capabilities and services to the nation's warfighters, national level leaders, and mission and coalition partners.

The DISA Director is also the Commander of the Joint Force Headquarters (JFHQ) DOD Information Network (DODIN) which maintains command and control (C2) of defensive cyber operations.

DISA delivers hundreds of IT support and service capabilities to our mission partners. Regardless of the IT service or support need, DISA has the capacity to host, support, engineer, test, or acquire IT services.

Additionally, in order to optimize DOD's world-class enterprise infrastructure, DISA is focused on providing enterprise services, unified capabilities and mobility options to support DOD operations anywhere, anytime. Through enterprise security architectures, smart computing options and other leading-edge IT opportunities, DISA remains committed to its role of the IT provider to meet our defense needs.

DISA has organized its workforce to optimally support and work with leaders and partners in the White House, Pentagon, military services, combatant commands, and defense and federal agencies, as well as, coalition partners across the globe.

Through the White House Communications Agency (WHCA), an agency special mission DISA provides direct telecommunications and IT support to the president, vice president, their staffs and the U.S. Secret Service.

DISA also has a significant presence in the Pentagon with a support cadre in the Joint Staff Support Center providing direct support to the chairman of the Joint Chiefs of Staff, the senior ranking member of the Armed Forces; the Joint Chiefs of Staff comprised of the senior ranking officers from each military service; and the Joint Staff.

The Joint Staff J6 for command, control, communications, computers/cyber (C4) represents the joint warfighter in support of C4 requirements validation and capability development processes while ensuring joint interoperability. The J6 also partners with DISA as the department evolves the Joint Information Environment (JIE) with the development and promulgation of enterprise services and the enhancement of the enterprise information infrastructure.

DISA has a field office co-located with and directly supporting each of the nine unified combatant commands: U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Northern Command, U.S. Pacific Command, U.S. Southern Command, U.S. Special Operations Command, U.S. Strategic Command, and U.S. Transportation Command. DISA also has a support element assigned to U.S. Cyber Command, a sub-unified command under U.S. Strategic Command.

DISA provides DOD IT support through its DOD Enterprise Computing Centers (DECC), Defense Information Technology Contracting Organization (DITCO) field sites, and special mission centers, such as the Joint Spectrum Center and Joint Interoperability Test Command. In addition, we operate the DISA Command Center, which maintains situational awareness of all network operations and the DISA-provided infrastructure, computing, and enterprise services. This center ensures continued quality customer service to all of DISA's mission partners.

Joint Information Environment (JIE): As the department evolves the Joint Information Environment, the lines between components will blur. The matrixed organization evolving the JIE illustrates the department's technological way ahead. The current organization includes the Joint Chiefs of Staff (JCS), Office of the Deputy Chief Management Officer (DCMO), DOD CIO, Joint Staff J6, USCYBERCOM, military services, intelligence community, and National Guard.

The management of JIE is conducted through the JIE Executive Committee, which is tri-chaired by the DOD CIO, Joint Staff J6, and the USCYBERCOM commander.

In execution, there are three lines of operation: governance, operations, and technical synchronization. DISA has been given responsibility for the technical aspects of JIE and leads the JIE Technical Synchronization Office (JTSO), which includes agency staff, as well as representation from the military services, intelligence community, and National Guard.

Source: http://www.disa.mil/About, accessed 17 May 2016.

IV. Joint Organizations

A. Joint Spectrum Center (JSC)

The Joint Spectrum Center (JSC), a field office within the Defense Spectrum Organization (DSO), has leading experts in the areas of spectrum planning, electromagnetic environmental effects (E3), information systems, modeling and simulation, and operations to provide complete, spectrum-related services to the military departments and combatant commands. JSC has extensive experience in applying electromagnetic environmental databases and analysis tools to assist in both the acquisition and operation of communications-electronics assets. JSC is a source of engineering expertise and services dedicated to ensuring effective use of the electromagnetic spectrum.

JSC provides services such as spectrum-planning guidance, system integration, system vulnerability analysis, environmental analysis, test and measurement support, operational support and spectrum management software development.

JSC provides support for spectrum planning, spectrum certification of new weapon and sensor system development, and training and operational support to the unified commands, military departments, and defense agencies. These services are also available to federal and local government activities. Additionally, foreign nations can obtain assistance through Foreign Military Sales (FMS) channels. JSC can provide these services to U.S. industries when the efforts are determined to be in the interest of national security.

JSC Divisions/Services:

Operational Support (J3) Operational Support (J3) provides communications-electronics and electromagnetic battlespace support, and joint spectrum interference resolution support to the Combatant Commands.

Electromagnetic Environmental Effects (E3) Engineering (J5) researches, assesses, and models emerging spectrum technologies; manages the DOD E3 program; provides E3 advice and training, responsible for EM and spectrum engineering related information, modeling, and simulation systems development, and serves as the Lead Standardization Activity for the DOD Electromagnetic Compatibility Standardization Area.

Information Systems (J6) provides efficient and effective information system and information assurance support to the DSO and JSC, enabling net-centric spectrum operations.

Applied Engineering Division (J8) Provide tailored engineering support and guidance that enables the DOD and military services to proactively plan, design, acquire, and operate spectrum-dependent systems compatibly in their intended electromagnetic environment.

Source: http://www.disa.mil/mission-support/spectrum/About-Us/Joint-Spectrum-Center, accessed 17 May 2016.

B. Joint Communications Support Element (JCSE)

The Joint Communications Support Element provides rapid, reliable, and interoperable communications that link the combined joint task force (CJTF) and staff to the President and SecDef, geographic combatant commanders (GCCs), their component headquarters (HQ), and multinational partners. JCSE tactical communication packages vary in capability from small initial-entry and early-entry teams to a significantly larger deployable joint C2 system. Packages can support operations worldwide as well as in homeland defense (HD) and defense support of civil authorities (DSCA) missions.

Mission: On order, JCSE immediately deploys to provide enroute, early entry, scalable C4 support to the GCCs, Special Operations Command (USSOCOM), and other agencies as directed; on order, provides additional C4 services within 72 hours to support larger JTF HQs across the full spectrum of operations.

Organization: JCSE is a Joint Command consisting of a Headquarters Support Squadron (HSS) and Communications Support Detachment (CSD) three active squadrons, two Air National Guard squadrons, one Army Reserve Squadron.

- The three active squadrons, 1st, 2nd, and 3rd Joint Communications Squadron (JCS) as well as HSS and CSD are all headquartered at MacDill AFB, near Tampa, FL.
- The Army Reserve Squadron or 4th JCS is also headquartered at MacDill AFB, FL.
- The Air National Guard Squadrons are part of the Florida and Georgia Air Guard:
  - The 290th Joint Communications Support Squadron (JCSS) is from the Florida Air Guard, and is headquartered at MacDill AFB, FL.
  - The 224th JCSS is from the Georgia Air Guard and is headquartered at Brunswick, GA.

Core Competencies: The Element's core competency – what makes us different – is our communications support for contingency operations as directed by the Transportation Command (USTRANSCOM). With us, you will see the latest technologies that meet today's operational requirements. We are a tactical unit that has a rare ability to operate at the tactical, operational, and strategic levels. As a part of our contingency mission, we provide enroute, initial entry, or early entry communications support for up to 40-personnel Joint Task Force in support of permissive and non-permissive environments.

Additionally, the Element has the requisite skill sets to support larger Joint Task Force (JTF) Headquarters and two Joint Special Operations Task Force (JSOTF) Headquarters – anywhere from 40 to 1500 users.

To meet this expansive mission requirement, JCSE maintains a professional force of trained, rapidly deployable communications experts who possess only the latest forms of network and telecommunications skills. Our diverse and flexible organization comprises both active and reserve component forces. We are the model of the total force and our units routinely exercise and deploy together, making for an effective team capable of accommodating a wide range of mission options and tasks.

Source: http://www.jcse.mil/index_n.htm, accessed 17 May 2016.

C. U.S. Cyber Command (USCYBERCOM)

On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM). Full Operational Capability (FOC) was achieved Oct. 31, 2010. The command is located at Fort Meade, MD.

Formal Command Name: U.S. Cyber Command (USCYBERCOM)

Commander: Admiral Michael S. Rogers

Mission: USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries.

Focus: The Command has three main focus areas: Defending the DODIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack.

The Command unifies the direction of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD's cyber expertise. USCYBERCOM improves DOD's capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM is designing the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute our assigned missions. The command also works closely with interagency and international partners in executing these critical missions.

Organization: USCYBERCOM is a sub-unified combatant command subordinate to USSTRATCOM. Its service elements include Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER) and Marine Forces Cyber Command (MARFORCYBER). Coast Guard Cyber Command (CGCYBER), although subordinate to the Department of Homeland Security, has a direct support relationship to USCYBERCOM. The Command is also standing up dedicated Cyber Mission Teams to accomplish the three elements of our mission.

Seal: The eagle, our national symbol, is revered for the keen eyesight that allows it to pierce the darkness and remain vigilant. The two swords on the shield represent the dual nature of the command to defend the nation and, if necessary, engage our enemies in the cyber domain. The lightning bolt symbolizes the speed of operations in cyber, and the key illustrates the command's role to secure our nation's cyber domain.

Source: https://www.stratcom.mil/factsheets/2/Cyber_Command/, accessed 17 May 2016.

V. Service Organizations

A. Army Cyber Command (ARCYBER) / 2nd Army

Army Cyber Command (ARCYBER) is an operational Army force reporting directly to HQDA. At the direction of the SecDef, the Secretary of the Army assigned ARCYBER to U.S. Strategic Command to function as the Army Force Component Headquarters of U.S. Cyber Command.

Second Army and its assigned elements comprise an Army force retained by the Secretary of the Army. Second Army is a Direct Reporting Unit of the CIO/G-6 in the execution of administrative, policy, management, architecture, and compliance responsibilities.

ARCYBER and Second Army's breadth of responsibility spans the entire Army and the entire world, from the tactical edge to the strategic enterprise level or national levels. Traditional boundaries no longer exist and anonymous attacks can occur literally at near-light speed over fiber optic networks. Our enemies will attempt to deny freedom of movement on our networks and use any resources they can, from anywhere on earth, to gain an advantage.

ARCYBER and Second Army is composed of a professional team of elite warriors defending Army networks and providing full-spectrum cyber capabilities, enabling mission command and providing our forces with a global advantage. Cyber warfighting requires impact, integration, risk, and knowing ourselves, our enemies, and the cyber terrain. We are the Army leader in operating, maintaining, and defending the network.

Mission. United States Army Cyber Command and Second Army directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

Roles. ARCYBER is the Army's proponent for cyberspace operations to improve all aspects of Army doctrine, organization, training, materiel, leadership, personnel, and facilities related to cyberspace operations.

- Serve as service component to U.S. Cyber Command
- Train, organize and equip - Provide trained & ready forces
- Defense of all Army networks
- Proponency for Army Cyber … develop requirements
- Develop Army cyberspace capabilities and capacities
- Integrate cyberspace into planning and exercises
- Prepare to act as a cyber Joint Task Force Commander
- "Operationalize" cyber for the Army

Organization. ARCYBER has more than 21,000 Soldiers, DA Civilians and Contractors working across the globe conducting a full range of cyberspace operations - 24/7/365. Army Cyber Command is a unified operations center responsible for all Army networks supported by:

- U.S. Army Network Enterprise Technology Command (NETCOM)
- U.S. Army Intelligence and Security Command (INSCOM)
- 1st Information Operations Command (Land)

Source: http://www.arcyber.army.mil/, accessed 17 May 2016.

B. Network Enterprise Technology Command (NETCOM)

Organization: The U.S. Army Network Enterprise Technology Command, headquartered at Fort Huachuca, Arizona, is the Army's single information technology service provider for all network communications. NETCOM plans, engineers, installs, integrates, protects, operates, maintains and defends the Army's Networks, enabling mission command through all phases of Joint, Interagency, Intergovernmental and Multinational operations. NETCOM has the expertise of more than 15,800 Soldiers and Civilians supporting every Army Command, Army Service Component Command and Direct Reporting Unit in more than 20 countries and everywhere there is an Army presence.

Mission: Install, engineer, operate and defend our Army's Network and Mission Command capabilities daily and through all phases of Joint, Interagency, Intergovernmental and Multinational operations. As directed, supports other national missions or contingency operations. In order to support freedom of action in the information environment and to deny the same to our adversaries.

Vision: The Army's Premier Global Command - a committed, innovative team and family accomplishing any mission, anywhere, anytime.

Subordinate Organizations:

5th Signal Command (Theater), headquartered at Lucius D. Clay Kaserne in Wiesbaden, Germany, is NETCOM's communications arm in Europe. Its mission is to build, operate, defend, and extend network capabilities to enable mission command and create tactical, operational, and strategic flexibility for Army, Joint, and Multi-national forces in the European Command and Africa Command areas of responsibility.

5th SC(T) provides and extends network capabilities through all operational phases for Warfighters, allowing continuous and transparent battle command. The 5th SC(T) manages the region's Joint Network Enterprise components, enabling the Global Network Enterprise for operating forces in Europe or those traversing through the theater. With approximately 3,000 Soldiers, Civilians and contractors, 5th SC(T) serves as the primary network provider to the two unified combatant commands and their formations.

The 7th Signal Command (Theater), headquartered at Fort Gordon, Georgia, installs, operates and defends Network and Mission Command capabilities for Joint, Interagency, Intergovernmental, and Multinational forces within the Western Hemisphere in support of Unified Land Operations.

As directed, the command also supports other national missions or contingency operations through three theater strategic signal brigades, the 2d Regional Cyber Center, the Army's Cyber Mission Brigade, and 44 Network Enterprise Centers at installations across the nation. The 7th SC(T) delivers critical Information Technology solutions, capabilities and services to approximately 80 percent of the Army, supporting warfighting, generating forces, and mission partners.

The 311th Signal Command (Theater), Headquartered at Fort Shafter, Hawaii, is the most geographically dispersed signal command in the Army with subordinate units stationed in California, Alaska, Hawaii, Japan, and Korea, employing more than 3,000 U.S. Army active-duty and Reserve Soldiers and Civilian personnel.

The 311th SC(T) executes and integrates expeditionary Command and Control capabilities to enable joint, coalition, and combined Command, Control, Communications, Computers and Intelligence support for the Army Service Component Commander and Pacific Combatant Commander. The mission of the 311th SC(T) is to plan, build, operate, defend,

and extend Army and Joint networks throughout the Pacific Theater to enable mission command for full spectrum, Joint, Interagency, Intergovernmental, and Multinational operations across all Joint operational phases. As directed, ensures U.S. and Allied freedom of action in cyberspace.

The 335th Signal Command (Theater) with nearly 8,000 Soldiers, is the largest multifunctional signal command in the U.S. Army Reserve, with its headquarters located in East Point, Georgia. The 335th SC(T) provides mission command for two tactical theater signal brigades, a chemical brigade and a regional support group.

The 335th SC(T) has four enhanced signal battalions, a combat camera company, a tactical installation/networking company and a joint communications squadron element as an Administrative Control unit. The 335th SC(T) also has an operational command post headquartered in Camp Arifjan, Kuwait, which provides the engineering and integration of the strategic and tactical network operations architecture for U.S. Army Central Command.

Source: http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/, accessed 17 May 2016.

C. Intelligence and Security Command (INSCOM)

Organization: INSCOM is an Army major command that conducts intelligence, security and information operations for military commanders and national decision makers.

Headquartered at Fort Belvoir, Virginia, INSCOM is a global command with major subordinate commands and a variety of smaller units with personnel dispersed over 180 locations worldwide.

Mission: INSCOM executes mission command of operational intelligence forces; conducts worldwide multi-discipline and all-source intelligence operations; delivers advanced skills training, linguist support, specialized quick reaction capabilities, and intelligence-related logistics, contracting, and communications in support of Army, Joint, and Coalition commands and the National Intelligence Community.

Subordinate Organizations:

1st Information Operations Command (Land): The 1st IO Command is the only Army full-spectrum IO organization engaged from information operations theory development and training to operational application across the range of military operations.

66th Military Intelligence Brigade: The 66th MI Brigade conducts theater level multidiscipline intelligence and security operations and, when directed, deploys prepared forces to conduct joint/combined expeditionary and contingency operations in support of U.S. Army Europe and U.S. European Command.

116th Military Intelligence Brigade: The 116th MI Brigade conducts 24/7 tasking, collection, processing, exploitation, dissemination and feedback of multiple organic and Joint intelligence aerial-intelligence surveillance and reconnaissance (A-ISR) missions collected in overseas contingency areas of operation.

300th Military Intelligence Brigade (Linguist): The 300th MI Brigade provides trained and ready linguist and military intelligence soldiers to commanders from brigade through Army level.

470th Military Intelligence Brigade: The 470th MI Brigade provides timely and fused multi-discipline intelligence in support of U.S. Army South, U.S. Southern Command and other national intelligence agencies.

500th Military Intelligence Brigade: The 500th MI Brigade, located at Schofield Barracks, Hawaii, provides multi-disciplined intelligence support for joint and coalition warfighters in the U.S. Army Pacific area of responsibility.

501st Military Intelligence Brigade: The 501st MI Brigade conducts theater-level multi-discipline intelligence for Joint and Combined Warfighters from the Republic of Korea.

513th Military Intelligence Brigade: The 513th MI Brigade deploys in strength or in tailored elements to conduct multidiscipline intelligence and security operations in support of Army components of U.S. Central Command, and theater Army commanders.

704th Military Intelligence Brigade: The 704th MI Brigade conducts synchronized full-spectrum signals intelligence, computer network and information assurance operations directly and through the National Security Agency to satisfy national, joint, combined and Army information superiority requirements.

706th Military Intelligence Group: The 706th MI Group, located at Fort Gordon, Ga., provides personnel, intelligence assets and technical support to conduct signals intelligence

operations within the National Security Agency/Central Security Service Georgia (NSA/CSS Georgia) and worldwide.

780th Military Intelligence Brigade: The 780th MI Brigade, located at Fort George G. Meade, Md., conducts signals intelligence, computer network operations, and enables Dynamic Computer Network Defense operations of Army and Defense networks.

902d Military Intelligence Group: The 902d MI Group provides direct and general counterintelligence support to Army activities and major commands.

Army Cryptologic Operations (ACO): ACO serves as the Army G2 and Service Cryptologic Component (SCC) representative to provide expert cryptologic leadership, support, guidance and advice to U.S. Army Warfighters and Intelligence leaders. Lead the Army's Cryptologic effort to satisfy Signals Intelligence (SIGINT) requirements by leveraging NSA Extended Enterprise, Intelligence Community, Sister Services and Service Laboratories. Ensure timely and effective support to operations by providing optimized capabilities, training and resources.

Army Field Support Center (AFSC): AFSC provides specialized operational, administrative and personnel management support to Department of the Army and other Department of Defense Services and Agencies as directed.

Army Operations Group (AOG): AOG conducts human intelligence operations and provide expertise in support of ground component priority intelligence requirements using a full spectrum of human intelligence collection methods.

Joint Surveillance Target Attack Radar System (JSTARS): Army JSTARS provides Army aircrew members aboard JSTARS aircraft to support surveillance and targeting operations of Army land component and joint or combined task force commanders worldwide.

National Ground Intelligence Center (NGIC): NGIC is the Defense Department's primary producer of ground forces intelligence.

Source: http://www.army.mil/inscom, accessed 17 May 2016.

D. 1st Information Operations Command (Land)

Organization: As a source of IO planning and integration expertise, the Command strives to think across inherent boundaries and gain an advantage through the coordinated use of multiple capabilities to affect the information environment. This Command does not operate exclusively in any of the IO competencies; it utilizes the synergy of multiple, simultaneous solutions needed throughout the U.S. Army and other Military Forces around the world.

Mission: 1st Information Operations Command (Land) provides IO and Cyberspace Operations support to Army and other Military Forces through:

- Deployable Support Teams
- Opposing forces support
- Reachback planning and analysis
- Specialized training

In order to support freedom of action in the information environment and to deny the same to our adversaries.

Unique Capabilities to Support the Warfighters: 1st IO Command provides Information Operations support to the Army and other Military Forces. Our functional areas include IO Intelligence, Reachback Teams, deployable IO Support Teams, and IO Training.

- Tailored IO Support Teams
- IO Vulnerability Assessments
- Cyber OPFOR
- Intelligence Support to IO
- Reachback Support
- Specialized IO Training (Mobile & Resident)
- OPSEC Support
- Cyberspace Operations Support
- IO Planning Support
- IO Best Practices
- IO Doctrine – Review
- Exercise Support

Key Functions:

- Cyberspace Opposing Force
- IO Planning Support
- Intelligence Support to IO
- OPSEC Support
- Specialized IO Training
- Vulnerability Assessments

Subordinate Organizations: 1st IO Command is comprised of two battalions. The 1st IO Battalion primarily provides IO Field Support Teams (FSTs), IO Vulnerability Assessment Teams (IOVATs), Army OPSEC support and training teams, and other missions. The 2d IO Battalion primarily provides Cyber Opposing Forces. The Command is a multi-component unit with an integrated U.S. Army Reserve Element.

1st Battalion: 1st Information Operations Battalion trains and deploys IO Teams to:

- Improve the supported unit's ability to plan, synchronize, integrate, and execute Information Operations;

- Conduct multi-disciplined Information Operations vulnerability assessments; and
- Provide OPSEC assistance and training,

in order to provide tactical to strategic level Information Operations support to Army units, Joint Forces, DOD organizations, and interagency efforts.

2d Battalion: 2d Information Operations Battalion executes cyberspace opposing force operations and provides cyberspace operational support to Army and other Military Forces; on order, conducts cyberspace operations to defend Army networks, enable freedom of action in the Information Environment and deny the same to adversaries.

Reserve Component Integration Section (RCIS): The Reserve Component Integration Section (RCIS) provides trained and ready Soldiers in support of 1st IO Command's global mission to operationally integrate information operations, defend cyberspace and provide reachback planning and analysis for Army and Joint stakeholders.

Headquarters and Headquarters Detachment (HHD): Headquarters and Headquarters Detachment provides Command and Control (C2), military justice, administration, training, and command logistics in support of 1st IO Command.

Leadership: The Commander of 1st IO Command is an Army Colonel who is qualified as a functional Area 30, Information Operations Officer. Battalion Commanders and key Brigade and Battalion staff are a mixture of FA-30, FA-53, Military Intelligence, Signal Corps, and other Branches and Functional Areas that represent the diverse skills and multi-component nature of the Command and its missions.

Source: https://www.1stiocmd.army.mil/Home/Index, accessed 17 May 2016.

E. Army Chief Information Officer/G-6 (CIO/G-6)

Mission: The CIO/G-6 leads Army network modernization to deliver timely, trusted and shared information for the Army and its mission partners.

Vision: A secure, integrated, standards-based environment that ensures uninterrupted global access and enables collaboration and decisive action throughout all operational phases across all environments.

Lines of Effort:

- Provide Signal Capabilities to the Force
- Enhance Cybersecurity Capabilities
- Increase Network Throughput & Ensure Sufficient Computing Infrastructure
- Deliver IT Services to the Edge
- Strengthen Network Operations

Role as CIO:

- Report Directly to the Secretary
- Set the Strategic Direction and Objectives for the Army Network
- Supervise all Army C4 and IT Functions
- Manage Enterprise IT Architecture
- Establish and Enforces IT Policies
- Directs Delivery of Operational C4IT Capabilities to Support Warfighting and Business Requirements
- Assess and Ensure Compliance of all IT and National Security Systems

Role as G6:

- Advise the Chief of Staff on Planning, Fielding, and Execution of Worldwide C4IT in Support of Army Operations
- Develop and Execute the Army's Network Strategy, Architecture, and Implementation Plan for the Global Enterprise Network
- Implement Army Information Assurance Activities
- Supervise C4IT, Signal Support, Information Security, Force Structure and Equipping Activities in Support of Warfighting Operations
- Oversee Management of the Signal Forces

Source: http://ciog6.army.mil/Home/tabid/36/Default.aspx, accessed 17 May 2016.

F. Marine Corps Forces Cyber (MARFORCYBER)

Marine Forces Cyberspace Command (MARFORCYBER) is engaging in ongoing cyberspace operations, making strong progress with the force build, achieving operational outcomes, and building capacity for tomorrow's opportunities and challenges. Our priorities are to operate and defend our networks, support designated COCOMs with full spectrum cyber operations, organize for the fight, train and equip the cyber workforce, develop workforce lifecycle management, and to ensure mission readiness through joint and service capabilities integration.

Mission: As the service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum Cyberspace Operations to ensure freedom of action in and through cyberspace, and deny the same to our adversaries.

Operations: The operations include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (DCO) within the MCEN and Department of Defense Information Networks (DODIN), and - when directed -conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. MARFORCYBER is also designated at the Joint Force Headquarters – Cyber (JFHQ–CYBER) as directed by USCYBERCOM.

Operationalizing Cyber: MARFORCYBER is in its sixth year of operation. Our focus remains developing ready cyberspace capability for the naval, joint and coalition force. Consistent with our Commandant's guidance, we are developing tactical cyber capacity as an organic aspect of how we fight.

Further, in conjunction with joint and interagency partners, we intend to pursue the development of an integrated and unified platform for cyberspace operations that will enable centralized command and control, real time situational awareness, and decision support. We are accomplishing this through close coordination with industry partners, and aligned with DOD and USCYBERCOM priorities in support of the Joint Information Environment.

Source: Statement by Major General Daniel J. O'Donohue, Commanding General Marine Forces Cyberspace Command, Before the House Armed Services Committee, 4 March 2015, http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-ODonohueD-20150304.pdf, accessed 17 May 2016.

G. Navy U.S. Fleet Cyber / U.S. TENTH Fleet (FCC-C10F)

Warfighters - First and foremost, the men and women who make up the U.S. Fleet Cyber Command/U.S. TENTH Fleet (FCC/C10F) team around the world are warriors who remain motivated and mission focused. FCC/C10F warfighters direct cyberspace operations to deter and defeat aggression while ensuring freedom of action in cyberspace. Operations are not limited to cyberspace alone, however, as FCC/C10F is the Navy's central operational authority for cryptologic/signals intelligence, information operations, electronic warfare, and space capabilities in addition to cyber and networks operations.

Operational - U.S. Fleet Cyber Command serves as the Navy component command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component commander under the National Security Agency/Central Security Service. Fleet Cyber Command also reports directly to the Chief of Naval Operations as an Echelon II command.

U.S. 10th Fleet is the operational arm of Fleet Cyber Command and executes its mission through a task force structure similar to other warfare commanders. In this role, C10F provides operational direction through its Maritime Operations Center located at Fort George Meade Md., executing command and control over assigned forces in support of Navy or joint missions in cyber/networks, information operations, electronic warfare, cryptologic/signals intelligence and space.

Strategy - Navy Cyber Power 2020 is the road map for continued success and requires U.S. Fleet Cyber Command/U.S. TENTH Fleet (FCC/C10F) to address cyber threats, key trends, and challenges across four main areas, which are (1) integrated operations, (2) an optimized cyber workforce, (3) technology innovation, and (4) reforming development and execution of our requirements, acquisition, and budgeting. The NCP 2020 vision is assured access to cyberspace and confident command and control, preventing strategic surprise in cyberspace, and delivering decisive cyber effects.

Cyber Norm - The new cyber norm is the reality in which we operate and requires the entire Navy team to constantly stay ahead of the adversary in the cyber arena. The Navy's network defenders must consistently and dynamically outpace the enemy, denying adversaries any benefit. As important, every user must understand their responsibility to also deny the enemy any advantage when on the network. After all, if the Navy has given you access to a keyboard, you are operating in the cyber domain.

With the stand-up of U.S. Fleet Cyber Command and re-commissioning of U.S. 10th Fleet in January 2010, the Navy recognized the need "...to confront a new challenge to our nation's security in cyberspace." Over the four years since then, as the Navy's culture has begun to change with respect to cyber in Joint warfighting, the necessity for an active cyber defense has become more and more apparent. Late summer of 2013, the Navy expanded its aggressive campaign to enhance the security of its networks. Since then and moving forward, we will continually apply defensive measures and architectural hardening improvements (making the network more defensible) to strengthen the security of our networks

Fleet Cyber Command

Mission: The mission of Fleet Cyber Command is to serve as central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore; to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to execute cyber missions as directed; to direct, operate, maintain, secure, and defend the

Navy's portion of the Department of Defense Information Networks (DODIN); to deliver integrated cyber, information operations, cryptologic, and space capabilities; to deliver a global Navy cyber common operational picture; to develop, coordinate, assess, and prioritize Navy cyber, cryptologic/signals intelligence, space, information operations, and electronic warfare requirements; to assess Navy cyber readiness; and to exercise administrative and operational control of assigned forces.

Vision: Fleet Cyber Command's vision is to conduct operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint/Coalition freedom of action and decision superiority while denying the same to our adversaries. We will win in these domains through our collective commitment to excellence and by strengthening our alliances with entities across the U.S. government, Department of Defense, academia, industry, and our foreign partners.

Tenth Fleet

Mission: The mission of Tenth fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.

Source: http://www.public.navy.mil/fcc-c10f/Pages/home.aspx, accessed 17 May 2016.

H. Air Forces Cyber / 24th Air Force

The 24th Air Force is the operational warfighting organization that establishes, operates, maintains and defends Air Force networks to ensure warfighters can maintain the information advantage as US forces prosecute military operations around the world.

On 6 October 2008, following its annual Corona conference, the U.S. Air Force announced that a numbered air force, the 24th Air Force, would gain the cyber warfare mission as part of Air Force Space Command. The 24th Air Force was activated on 18 August 2009, achieved Initial Operating Capability in January 2010, and Full Operational Capability on 1 October 2010. On 7 December 2010, HQ 24th Air Force was re-designated Air Forces Cyber (AFCYBER) to recognize its role as the service component to United States Cyber Command.

More than 5,400 men and women conduct or support 24-hour operations involving cyberspace operations for 24th Air Force, including approximately 3,500 military, 800 civilian and 900 contractor personnel. Approximately 11,000 Air Reserve Component personnel came to AFSPC from existing Air Force Reserve and Air National Guard units associated with the combat communications mission of the 689th Combat Communications Wing and the Air Force Network Operations mission of the 67th Network Warfare Wing.

Mission: The mission of the 24th Air Force is to extend, operate and defend the Air Force portion of the Department of Defense network and provide full spectrum capabilities for the Joint warfighter in, through and from cyberspace.

Organization: The 24th Air Force is comprised of an integrated operations center and three wings located at Lackland AFB, TX, and at Robins Air Force Base, GA.

> **624th Operations Center's** mission is to establish, plan, direct, coordinate, assess, command and control full spectrum cyberspace operations and capabilities in support of Air Force and Joint requirements.
>
> **67th Cyberspace Wing** is charged as the Air Force execution element for Air Force Network Operations and providing network warfare capabilities to Air Force, Joint Task Force and combatant commanders that operate, manage and defend global Air Force networks.
>
> **688th Cyberspace Wing** is responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter information technology, strategy, tactics and data to control the information battlespace and provide the world's best IO leaders.
>
> **The 689th Combat Communications Wing** trains, deploys and delivers to the President, Secretary of Defense, the Combatant Commanders and the warfighter expeditionary communications, information systems, engineering and installation, air traffic control and weather services.

Source: http://www.24af.af.mil/About-Us/Fact-Sheets/Display/Article/458567/24th-air-force-fact-sheet, accessed 17 May 2016.

Glossary

Most terms are taken from the Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms* (8 Nov 2010, as amended through 15 Feb 2016). Other cyberspace terms are taken from *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02 (15 August 2005).

area of responsibility (AOR) — The geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations.

battle damage assessment (BDA) — The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force.

CERF — Cyber Effects Request Form.

CJCS — Chairman of the Joint Chiefs of Staff.

CMT — Combat Mission Team.

CCDR — Combatant Commander.

CCMD — Combatant Command.

command and control (C2) — The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

commander's critical information requirement (CCIR) An information requirement identified by the commander as being critical to facilitating timely decision making.

concept of operations (CONOPS) — A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources

counterintelligence (CI) — Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

course of action (COA) — 1. Any sequence of activities that an individual or unit may follow. 2. A scheme developed to accomplish a mission. 3. A product of the course-of-action development step of the joint operation planning process.

CPT — Cyberspace Protection Team.

cybersecurity — Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

cyberspace operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

cyberspace superiority — The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.

data mining — A method of using computers to sift through personal data, backgrounds to identify certain actions or requested items.

defensive cyberspace operations (DCO) — 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.

defensive cyberspace operations internal defensive measures (DCO-IDM) — Deliberate, authorized defensive measures or activities conducted within the Department of Defense information networks. They include actively hunting for advanced internal threats as well as the internal responses to these threats.

defensive cyberspace operations response actions (DCO-RA) — Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems.

denial of service attack (DOS) — A cyber attack designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

Department of Defense information networks (DODIN) — The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

DISA — Defense Information Systems Agency.

distributed denial of service attack (DDOS) — A cyber attack involving the use of numerous computers flooding the target simultaneously. Not only does this overload the target with more requests, but having the denial of service attack from multiple paths makes backtracking the attack extremely difficult, if not impossible. Many times worms are planted on computers to create zombies that allow the attacker to use these machines as unknowing participants in the attack.

DOD — Department of Defense.

DOD Information Network (DODIN) Operations — 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.

electromagnetic spectrum (EMS) — The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands.

electromagnetic spectrum management — Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures.

electronic attack (EA) — Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

electronic warfare (EW) — Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

e-mail spoofing — A method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source.

execute order (EXORD) — 1. An order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations. 2. An order to initiate military operations as directed.

firewall — A barrier to keep destructive forces away from your property.

GCC — Geographic Combatant Commander.

hacker — Advanced computer users who spend a lot of time on or with computers and work hard to find vulnerabilities in IT systems.

hacktivist — These are combinations of hackers and activists. They usually have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counterinformation or disinformation.

information environment — The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

information operations (IO) — The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

IPR — in-progress review.

intelligence — 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities.

intelligence requirement (IR) — 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces.

intelligence, surveillance, and reconnaissance (ISR) — An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

J-1 — manpower and personnel directorate of a joint staff; manpower and personnel staff section.

J-2 — intelligence directorate of a joint staff; intelligence staff section.

J-3 — operations directorate of a joint staff; operations staff section.

J-4 — logistics directorate of a joint staff; logistics staff section.

J-5 — plans directorate of a joint staff; plans staff section.

J-6 — communications system directorate of a joint staff; command, control, communications, and computer systems staff section.

JCC — Joint Cyberspace Center.

JFHQ-C — Joint Force Headquarters–Cyberspace.

JFHQ-DODIN — Joint Force Headquarters-Department of Defense Information Networks.

joint fires element (JFE) — An optional staff element that provides recommendations to the operations directorate to accomplish fires planning and synchronization.

joint force commander (JFC) — A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force.

joint integrated prioritized target list (JIPTL) — A prioritized list of targets approved and maintained by the joint force commander.

joint intelligence preparation of the operational environment (JIPOE) — The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process.

joint operation planning process (JOPP) — An orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint operation plan or order.

joint operations area (JOA) — An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission.

joint target list (JTL) — A consolidated list of selected targets, upon which there are no restrictions placed, considered to have military significance in the joint force commander's operational area.

joint targeting coordination board (JTCB) — A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance, synchronization, and priorities, and refining the joint integrated prioritized target list.

joint task force (JTF) — A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander.

keylogger — A software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard.

line of effort (LOE) — In the context of joint operation planning, using the purpose (cause and effect) to focus efforts toward establishing operational and strategic conditions by linking multiple tasks and missions.

line of operation (LOO) — A line that defines the interior or exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s).

logic bomb — A program routine that destroys data by reformatting the hard disk or randomly inserting garbage into data files.

malware (short for malicious software) — software designed specifically to damage or disrupt a system, such as a virus or a Trojan Horse.

measure of effectiveness (MOE) — A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.

measure of performance (MOP) — A criterion used to assess friendly actions that is tied to measuring task accomplishment.

military deception (MILDEC) — Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

military information support operations (MISO) — Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

navigation warfare (NAVWAR) — Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations.

Non-Secure Internet Protocol Router Network (NIPRNET) — The network used Department of Defense.

offensive cyberspace operations (OCO) — Cyberspace operations intended to project power by the application of force in or through cyberspace.

operation order (OPORD) — A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation.

operation plan (OPLAN) — 1. Any plan for the conduct of military operations prepared in response to actual and potential contingencies. 2. A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data.

operational environment (OE) — A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.

operational preparation of the environment (OPE) — The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment.

reachback — The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed.

rules of engagement (ROE) — Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered.

SECRET Internet Protocol Router Network — The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry.

signals intelligence (SIGNT) — 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals.

sniffers — A program designed to assist hackers/and or administrators in obtaining information from other computers or monitoring a network. The program looks for certain information and can either store it for later retrieval or pass it to the user.

spam — The unsolicited advertisements for products and services over the internet, which experts estimate to comprise roughly 50 percent of the e-mail.

spyware — Any technology that gathers information about a person or organization without their knowledge. Spyware can get into a computer as a software virus or as the result of installing a new program. Software designed for advertising purposes, known as adware, can usually be thought of as spyware as well because it invariably includes components for tracking and reporting user information.

special operations forces (SOF) — Those Active and Reserve Component forces of the Services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations.

TTP — tactics, techniques, and procedures.

time-sensitive target (TST) — A joint force commander validated target or set of targets requiring immediate response because it is a highly lucrative, fleeting target of opportunity or it poses (or will soon pose) a danger to friendly forces.

trojan horse — A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed performs a function in the background such as allowing other users to have access to your computer or sending information from your computer to other computers.

virus — A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program.

worm — A destructive software program containing code capable of gaining access to computers or networks and once within the computer or network causing that computer or network harm by deleting, modifying, distributing, or otherwise manipulating the data.

zombie — A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a distributed denial of service attack (DDOS).

The Dictionary of Military and Associated Terms is available on line at:
http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Endnotes

[1] General Joseph F. Dunford, "Meeting Today's Global Security Challenges with General Joseph F. Dunford," 29 March 2016, linked from *Center for Strategic and International Studies Home Page*, http://csis.org/files/attachments/160329_Meeting_Today%27s_Global_Security_Challenges_with_General_Joseph_F_Dunford.pdf (accessed 1 April 2016).

[2] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, 8 Nov 2010, as amended through 15 Feb 2016), 58.

[3] Brett T. Willliams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73, (2nd Quarter 2014): 12.

[4] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, 11 August 2011), ix.

[5] JP 5-0, III-1.

[6] JP 5-0, xv.

[7] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12(R) (Washington, DC: U.S. Joint Chiefs of Staff, 5 February 2013), vi and IV-1.

[8] JP 5-0, xix-xx.

[9] JP 5-0, III-7.

[10] JP 5-0, III-3.

[11] JP 5-0, xx.

[12] JP 5-0, xx-xxi.

[13] U.S. Joint Chiefs of Staff, *Planner's Handbook for Operational Design*, (Washington, DC: U.S. Joint Chiefs of Staff, 7 October 2011), V-9.

[14] JP 5-0, III-11 – 12.

[15] Planner's Handbook for Operational Design, V-13.

[16] Planner's Handbook for Operational Design, VI-1 – 2.

[17] "Fact Sheet: Department of Defense Cyber Strategy," linked from *U.S. Department of Defense Home Page*, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf 1 (accessed 1 April 2016).

[18] U.S. Joint Chiefs of Staff, *Cross Domain Synergy in Joint Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, 14 January 2016), 49-50.

[19] JP 3-12(R), I-4.

[20] Benjamin C. Leitzel, *Cyber Ricochet: Risk Management and Cyberspace Operations*, Issue Paper (Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, July 2012).

[21] Cross Domain Synergy in Joint Operations, 50-52.

[22] JP 3-12(R), I-3.

[23] U.S. Army, *Intelligence Preparation of the Battlefield/Battlespace*, Army Techniques Publication 2-01.3 / Marine Corps Reference Publication 2-3A (Washington DC: Headquarters Department of the Army, November 2014), 9-12.

[24] "Department of Defense Cyber Strategy," linked from U.S. Department of Defense Home Page, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed 1 April 2016), 9.

[25] JP 3-12(R), I-6 – 7.

[26] U.S. Air Force, *Cyberspace Operations*, Annex 3-12 (Maxwell AFB, AL: U.S. Air Force, 30 November 2011), 3-4.

[27] DOD Cyber Strategy, 10.

[28] "Manning guilty of 20 specifications, but not 'aiding enemy'," linked from *U.S. Army Home Page*, http://www.army.mil/article/108143/Closing_arguments_heard_in_Pfc__Manning_trial/ (accessed 1 April 2016).

[29] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/news/stories/2016/march/iranians-charged-with-hacking-us-financial-sector (accessed 1 April 2016).

[30] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/news/stories/2016/march/two-from-syrian-electronic-army-added-to-cybers-most-wanted/two-from-syrian-electronic-army-added-to-cybers-most-wanted (accessed 1 April 2016).

[31] "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," linked from *Department of Justice Home Page*, https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive (accessed 1 April 2016).

[32] "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities," linked from *Department of Justice Home Page*, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated (accessed 1 April 2016).

[33] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/wanted/cyber/huang-zhenyu/view (accessed 1 April 2016).

[34] "Justice Department Statement on the Request to Hong Kong for Edward Snowden's Provisional Arrest," linked from *Department of Justice Home Page,* https://www.justice.gov/opa/pr/justice-department-statement-request-hong-kong-edward-snowden-s-provisional-arrest (accessed 1 April 2016).

[35] Senator Tom Coburn, *The Federal Government's Track Record on Cybersecurity and Critical Infrastructure*, A report prepared by the Minority Staff of the Homeland Security and Governmental Affairs Committee (Washington, DC, 4 February 2014), 2.

[36] James R. Clapper, Director of National Intelligence, *Statement for the Record Worldwide Cyber Threats*, House Permanent Select Committee on Intelligence (Washington, DC, 10 September 2015), 3.

[37] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 4.

[38] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 2.

[39] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 2.

[40] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/wanted/cyber/firas-dardar (accessed 1 April 2016).

[41] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 2.

[42] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 4.

[43] Syrian Electronic Army Claims Hack of Army Website, 8 June 2016, linked from *Nexgov Home Page*, http://www.nextgov.com/defense/2015/06/syrian-electronic-army-claims-hack-army-website/114784/ (accessed 1 April 2016).

[44] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 2.

[45] Ellen Nakashima, Chinese government has arrested hackers it says breached OPM database, linked from The *Washington Post Home Page*, 2 December 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html (accessed 1 April 2016).

[46] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 4.

[47] Former U.S. Nuclear Regulatory Commission Employee Pleads Guilty to Attempted Spear-Phishing Cyber-Attack on Department of Energy Computers, linked from *Department of Justice Home Page*, https://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear-phishing-cyber (accessed 1 April 2016).

[48] Admiral Michael S. Rogers, Commander United States Cyber Command, *Statement Before the Senate Armed Services Committee* (Washington, DC, 5 April 2016), 5.

[49] U.S. Army, *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02 (Fort Leavenworth, KS: US Army Training and Doctrine Command, 15 Aug 2005), II-8 – 11.

[50] JP 3-12(R), I-7 – 8.

[51] U.S. Department of Defense, *DOD Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: U.S. Department of Defense, January 2013) cover memo and 17-18.

[52] JP 3-12(R), II-2 – 4.

[53] U.S. Army, Cyber Electromagnetic Activities, Field Manual 3-38 (Washington DC: Headquarters Department of the Army, February 2014), 3-5.

[54] FM 3-38, 3-4 – 5.

[55] JP 3-12(R), II-4 – 5.

[56] JP 3-12(R), I-5 and II-1.

[57] JP 5-0, xv.

[58] JP 5-0, IV-2.

[59] JP 5-0, xxv – xxvii.

[60] JP 3-12(R), IV-1.

[61] FM 3-38, 6-2 – 8.

[62] JP 3-13, II-9.

[63] Cross Domain Synergy in Joint Operations, 55-56.

[64] JP 3-12(R), IV-7.

[65] U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication 6-0 (Washington, DC: U.S. Joint Chiefs of Staff, 10 June 2015), III-5.

[66] The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects Power Projection through Cyberspace, 88.

[67] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," JFQ 73, 16.

[68] FM 3-38, 6-10.

[69] JP 5-0, III-20 – 22.

[70] JP 3-12(R), II-10 – 11.

[71] U.S. Army, *U.S. Army Report and Message Formats*, Field Manual 6-99 (Washington DC: Headquarters Department of the Army, August 2013), A-74 – 75.

[72] JP 5-0, xvi.

[73] U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication 3-33 (Washington, DC: U.S. Joint Chiefs of Staff, 30 July 2012), IX-9

[74] JP 5-0, 2-17 – 19.

[75] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, 11 August 2011), IV-6.

[76] U.S. Army, *Mission Command*, Army Doctrine Publication (ADP) 6-0, Change 2 (Washington, DC: Headquarters Department of the Army, 12 March 2014), 1-2.

[77] JP 3-0, III-22.

[78] JP 3-12(R), IV-4 – 5.

[79] JP 5-0, III-44.

[80] JP 3-0, 2-9 – 10.

[81] JP 3-12(R), I-8.

[82] JP 3-12(R), IV-6 – 7.

[83] U.S. Army, *Mission Command*, Army Doctrine Publication (ADP) 6-0, Change 2 (Washington, DC: Headquarters Department of the Army, 12 March 2014), 10-11.

[84] JP 3-12(R), IV-9 – 10.

[85] JP 3-12 (R), IV-3.

[86] Jason M. Gargan, "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects Power Projection through Cyberspace," *Air and Space Power Journal* 30, no. 1 (Spring 2016): 88.

[87] Lieutenant Commander Kallie D. Fink, Major John D. Jordan, and Major James E. Wells, "Considerations for Offensive Cyberspace Operations," *Military Review* (May-June 2014): 7-8.

[88] JP 3-12 (R), IV-3.

[89] Fink, Jordan, and Wells, "Considerations for Offensive Cyberspace Operations," 8 - 9.

[90] JP 3-12(R), IV-1 – 4.

[91] JP 3-12(R), IV-4 – 5.

[92] JP 3-12(R), IV-14.

[93] JP 3-12(R), III-2.

[94] JP 3-12(R), III-3.

[95] JP 3-12(R), IV-11 – 12.

[96] JP 3-12(R), I-7.

[97] Barrack Obama, President of the USA, *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, 13 February 2015, Stanford University, Stanford, CA.

[98] JP 3-27 Homeland Defense 29 July 2013, I-1 – 3.

[99] Critical Infrastructure Sectors, linked from the *Department of Homeland Security Home Page*, https://www.dhs.gov/critical-infrastructure-sectors (accessed 1 April 2016).

[100] DOD Protected Critical Infrastructure Program, linked from *Under Secretary of Defense for Policy Home Page*, http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram.aspx (accessed 1 April 2016).

[101] *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), 14.

[102] U.S. Joint Chiefs of Staff, *Homeland Defense*, Joint Publication 3-27 (Washington, DC: U.S. Joint Chiefs of Staff, 29 July 2013), II-2 – 3.

[103] JP 3-27, II-13.

[104] JP 3-27, II-8.

[105] JP 3-27, II-10.

[106] Admiral Michael S. Rogers, *Statement Before the Senate Armed Services Committee* (5 April 2016), 6-8.

[107] DOD Cyber Strategy, 2.

[108] JP 3-12(R), III-1 – 2.

[109] DOD Cyber Strategy, 10-11.

[110] DOD Cyber Strategy, 22-23.

[111] JP 3-12(R), III-2.

[112] DOD Cyber Strategy, 23.

[113] JP 3-12(R), I-8.

[114] JP 3-12(R), III-10.

[115] Cross Domain Synergy in Joint Operations, 4.

[116] E. Lincoln Bonner III, Cyber Power in 21st-Century Joint Warfare, *Joint Force Quarterly* 74 (3rd Quarter 2014): 105.

[117] Cross Domain Synergy in Joint Operations, 4.

[118] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 104-105.

[119] JP 6-0, ix.

[120] JP 6-0, I-7.

[121] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 106.

[122] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 105.

[123] Secretary of State John Kerry, "An Open and Secure Internet: We Must Have Both," Korea University, Seoul, Republic of Korea, 18 May 2015, linked from *Office of the Coordinator For Cyber Issues (S/CCI) Home Page*, http://www.state.gov/documents/organization/255014.pdf (accessed 1 April 2016)

[124] Secretary of State John Kerry, "An Open and Secure Internet: We Must Have Both."

This Page Intentionally Blank

CENTER for STRATEGIC LEADERSHIP
CSL