United States Army War College

Strategic Cyberspace Operations Guide

30 November 2018

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.

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 **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 planning process (JPP) detailed in Joint Publication 5-0, *Joint Planning* and applies these principles to the cyberspace domain found in Joint Publication 3-12, *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 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 policies, strategies, and guidance.

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. Gregory Hillebrand.

4. Changes from the third volume (dated 31 July 2018) include the 2018 National Cyber Strategy and Department of Defense Cyber Strategy as well as the Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA).

5. 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: Strategic Concepts and Doctrine Division
650 Wright Avenue
Carlisle, PA 17013

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 planning process (JPP) 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.[3]

2. The President, Secretary of Defense (SecDef), and Chairman of the Joint Chiefs of Staff (CJCS) use strategic direction to communicate their broad goals and issue-specific guidance to the Department of Defense (DOD). It provides the common thread that integrates and synchronizes the planning activities and operations of the Joint Staff, Combatant Commands (CCMDs), Services, joint forces, combat support agencies (CSAs), and other DOD agencies.[4] At the operational level, once strategic guidance is given, planning translates this guidance into specific activities aimed at achieving strategic and operational-level objectives and attaining the military end state.[5]

3. Combatant commanders (CCDRs) use strategic guidance and direction to prepare command strategies, focused on their command's specific capabilities and missions to link national strategic guidance to theater or functional strategies and joint operations. The command strategy, like national strategy, identifies broad, long-range objectives the command aims to achieve as their contribution toward national security. Plans translate the strategy into operations with the expectation that successful operations achieve the desired strategic objectives.[6]

4. Under the authorities of the SecDef, DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation.[7] Actions in cyberspace, through carefully controlled cascading effects, can enable freedom of action for activities in the physical domains.[8] CCDRs and Services use CO to create effects in and through cyberspace in support of military objectives.[9] The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the operational environment (OE).[10]

Intentionally Blank

Chapter 2: Design

I. Operational Design

1. Joint Publication 5-0, *Joint Planning*, describes operational design and the joint planning process (JPP). Operational design is a methodology to aid commanders and planners in organizing and understanding the operational environment (OE). The framework is built upon an iterative process that creates a shared understanding of the OE; identifies and frames problems within that OE; and develops approaches, through the application of operational art, to resolving those problems, consistent with strategic guidance and/or policy. The purpose of operational design and operational art is to produce an operational approach, allowing the commander to continue planning, translating broad strategic and operational concepts into specific missions and tasks and produce an executable plan.[11]

a. There are four major components to operational design (see Figure 2-1). The components have characteristics that exist outside of each other and are not necessarily sequential. However, an understanding of the OE and problem must be established prior to developing operational approaches. The process is continuous and cyclical in that it is conducted prior to, during, and for follow-on joint operations.

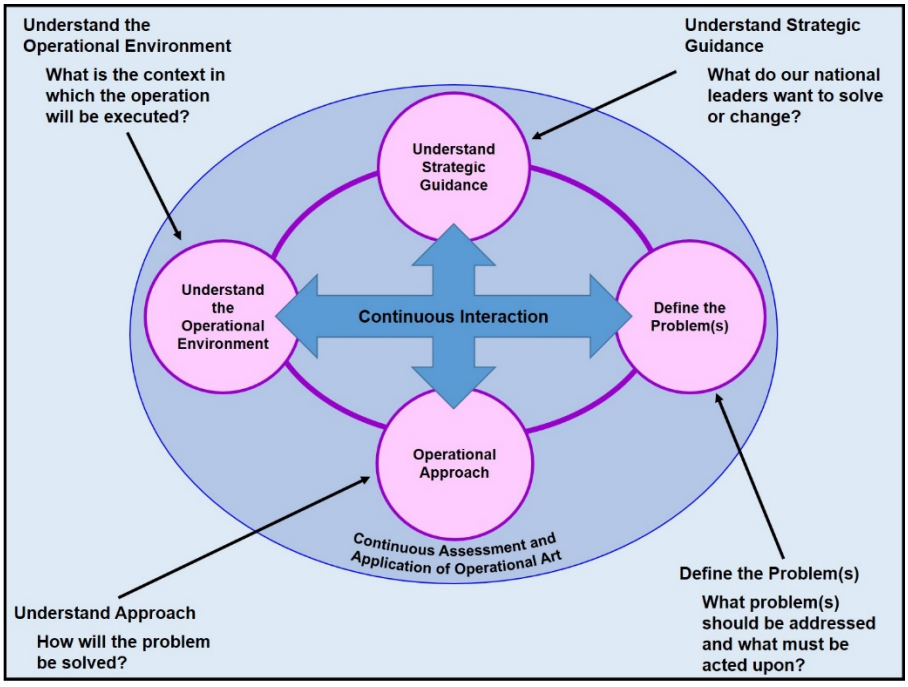

Figure 2-1: Operational Design Framework[12]

b. The general methodology in operational design is:

(1) Understand the strategic direction and guidance.

(2) Understand the strategic environment (policies, diplomacy, and politics).

(3) Understand the OE.

(4) Define the problem.

(5) Identify assumptions needed to continue planning (strategic and operational assumptions).

(6) Develop options (the operational approach).

(7) Identify decisions and decision points (external to the organization).

(8) Refine the operational approach(es).

(9) Develop planning guidance.[13]

II. Strategic Direction and Cyberspace.

1. The President, Secretary of Defense (SecDef), and Chairman of the Joint Chiefs of Staff (CJCS) 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 identify available forces, resources, and authorities (**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, although policy or national positions may limit options available to the commander. Connecting resources and tactical actions to strategic ends is the responsibility of the operational commander.[14]

2. **National Security Strategy**: In December 2017, President Trump issued the National Security Strategy of the United States of America (NSS). This document lays out a strategic vision for protecting the American people and preserving our way of life; promoting our prosperity; preserving peace through strength; and advancing American influence in the world.[15]

a. In order to protect the American people, the homeland, and the American Way of Life, the NSS lists five priority actions to "Keep America Safe in the Cyber Era:"

(1) Identify and Prioritize Risk: To improve the security and resilience of our critical infrastructure, we will assess risk across six key areas: national security, energy and power, banking and finance, health and safety, communications, and transportation.

(2) Build Defensible Government Networks: We will use the latest commercial capabilities, shared services, and best practices to modernize our Federal information technology.

(3) Deter and Disrupt Malicious Cyber Actors: The Federal Government will ensure that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities to prevent attacks before they affect or hold at risk U.S. critical infrastructure.

(4) Improve Information Sharing and Sensing: The U.S. Government (USG) will work with our critical infrastructure partners to assess their informational needs and to reduce the barriers to information sharing, such as speed and classification levels.

(5) Deploy Layered Defenses: Since threats transit globally, passing through communications backbones without challenge, the USG will work with the private sector to remediate known bad activities at the network level to improve the security of all customers.[16]

b. A second NSS pillar is to promote American prosperity. This pillar includes several cyberspace initiatives:

(1) Improvements in bandwidth, better broadband connectivity, and protection from persistent cyberattacks are needed to support America’s future growth and rejuvenate the Domestic Economy.

(2) Cybersecurity must be enhanced to protect the U.S. National Security Innovation Base (NSIB).

(3) To ensure energy security, the United States will work with allies and partners to protect global energy infrastructure from cyber and physical threats.[17]

c. To preserve peace through strength, the NSS directs three Cyberspace priority actions:

(1) Improve Attribution, Accountability, and Response: We will invest in capabilities to support and improve our ability to attribute cyberattacks, to allow for rapid response.

(2) Enhance Cyber Tools and Expertise: We will improve our cyber tools across the spectrum of conflict to protect U.S. Government assets and U.S. critical infrastructure, and to protect the integrity of data and information. U.S. departments and agencies will recruit, train, and retain a workforce capable of operating across this spectrum of activity.

(4) Improve Integration and Agility: We will improve the integration of authorities and procedures across the USG so that cyber operations against adversaries can be conducted as required. We will work with the Congress to address the challenges that continue to hinder timely intelligence and information sharing, planning and operations, and the development of necessary cyber tools.[18]

d. Finally, the NSS calls for advancing American influence. This objective can be achieved through multilateral forums to:

(1) Ensure Common Domains Remain Free: The United States will provide leadership and technology to shape and govern common domains — space, cyberspace, air, and maritime — within the framework of international law.

(2) Protect a Free and Open Internet: The United States will advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services.[19]

3. **National Defense Strategy**: In January 2018, the Department of Defense (DOD) published an unclassified synopsis of the classified 2018 National Defense Strategy (NDS) that articulates our strategy to compete, deter, and win in this environment.[20]

a. The strategic environment is competitive and complex:

(1) Today, every domain is contested — air, land, sea, space, and cyberspace.

(2) The homeland is no longer a sanctuary. America is a target of malicious cyber activity against personal, commercial, or government infrastructure. Increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.[21]

b. DOD's strategic approach includes building a more lethal force by investing in:

(1) Cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.

(2) Resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same

advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.[22]

4. **Defense Cyber Strategy**: In September 2018, DOD updated the Department of Defense Cyber Strategy (see Appendix A for cyberspace policies, strategies, and guidance).

a. The strategy defines five cyberspace objectives:

(1) Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;

(2) Strengthening the Joint Force by conducting cyberspace operations that enhance the U.S. military advantages;

(3) Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident

(4) Securing DOD information and systems against malicious cyber activity, including DOD information on non-DOD-owned networks; and

(5) Expanding DOD cyber cooperation with interagency, industry, and international partners.

b. The strategy defines five strategic approaches:

(1) Build a more lethal Joint Force

(2) Compete and deter in cyberspace

(3) Strengthen alliances and attract new partnerships

(4) Reform the Department

(5) Cultivate talent[23]

III. Cyberspace Strategic Environment.

1. After analyzing the strategic guidance, commanders and planners build an understanding of the strategic environment. This forms boundaries within which the operational approach must fit. Some considerations are:

a. What actions or planning assumptions will be acceptable given the current U.S. policies and the diplomatic and political environment?

b. What impact will U.S. activities have on third parties (focus on military impacts but identify possible political fallout)?

c. What are the current national strategic objectives of the USG? Are the objectives expected to be long lasting or short-term only? Could they result in unintended consequences (e.g., if you provide weapons to a nation, is there sufficient time to develop strong controls so the weapons will not be used for unintended purposes)?[24]

2. Within the OE, there are strategic-level considerations that may include global aspects due to global factors such as international law, the capability of adversary/enemy information activities to influence world opinion, adversary and friendly organizations and institutions, and the capability and availability of national and commercial space-based systems and information technology.[25]

3. **Policy and Strategy for Deterring Malicious Cyber Activities**. In response to the President's 11 May 2017 Executive Order 13800 on *Strengthening the Cybersecurity of Federal*

Networks and Critical Infrastructure, the Department of State (DOS) drafted a report that included a strategy and policies for deterring malicious cyber activities:

> a. The United States remains in a strong position to deter cyber attacks that would constitute a use of force because traditional tools of deterrence – including the responsive use of kinetic force – remain effective and potent. However, there are significant challenges in deterring the substantial increase in malicious state-sponsored cyber activity occurring below the threshold of the use of force.
>
> b. Deterrence by denial through defense and protection of critical infrastructure and other sensitive computer networks and ensuring efficient mitigation and timely recovery from malicious cyber activities must be foundational to the U.S. deterrence approach.
>
> c. The desired end states of U.S. deterrence efforts will be:
>
> > (1) A continued absence of cyber attacks that constitute a use of force against the United States., its partners, and allies.
> >
> > (2) A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force.
>
> d. Key elements of the approach will include:
>
> > (1) Creating a policy for when the United States will impose consequences.
> >
> > (2) Developing a range of consequences.
> >
> > (3) Conducting policy planning for imposing these consequences.
> >
> > (4) Building partnerships.[26]

IV. Cyberspace Operational Environment.

1. 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 OE 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.[27]

2. 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.[28]

3. **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"[29] in which cyber activities are turned against the originator or other unintended targets 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 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 cyber attack 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 their 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.[30]

h. **Layers**: Cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona (see Figure 2-2). Each layer represents a different focus from which Cyberspace Operations (CO) may be planned, conducted, and assessed.

(1) The **physical network layer** consists of the information technology (IT) devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components. The physical network components include the hardware and infrastructure (e.g., computing devices, storage devices, network devices, and wired and wireless links). Every physical component of cyberspace is owned by a public or private entity, which can control or restrict access to their components. These unique characteristics of the OE must be taken into consideration during all phases of planning.

(2) The **logical network layer** consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data). Individual links and nodes are represented in the logical layer but so are various distributed elements of cyberspace, including data, applications, and network processes not tied to a single node. An example is the Joint Knowledge Online Website, which exists on multiple servers in multiple locations in the physical domains but is represented as a single URL [uniform resource locator] on the World Wide Web.

(3) The **cyber-persona layer** is a view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another. Cyber-personas may relate directly to an actual person or entity. One individual may create and maintain multiple cyber-personas through use of multiple identifiers in cyberspace, such as separate work and personal email addresses, and different identities on different Web forums, chat rooms, and social networking sites, which may vary in the degree to which they are factually accurate. Conversely, a single cyber-persona can have multiple users, such as multiple hackers using the same malicious software (malware) control alias, multiple extremists using a single bank account, or all members of the same organization using the same e-mail address. The use of cyber-personas can make attributing responsibility for actions in cyberspace difficult.[31]

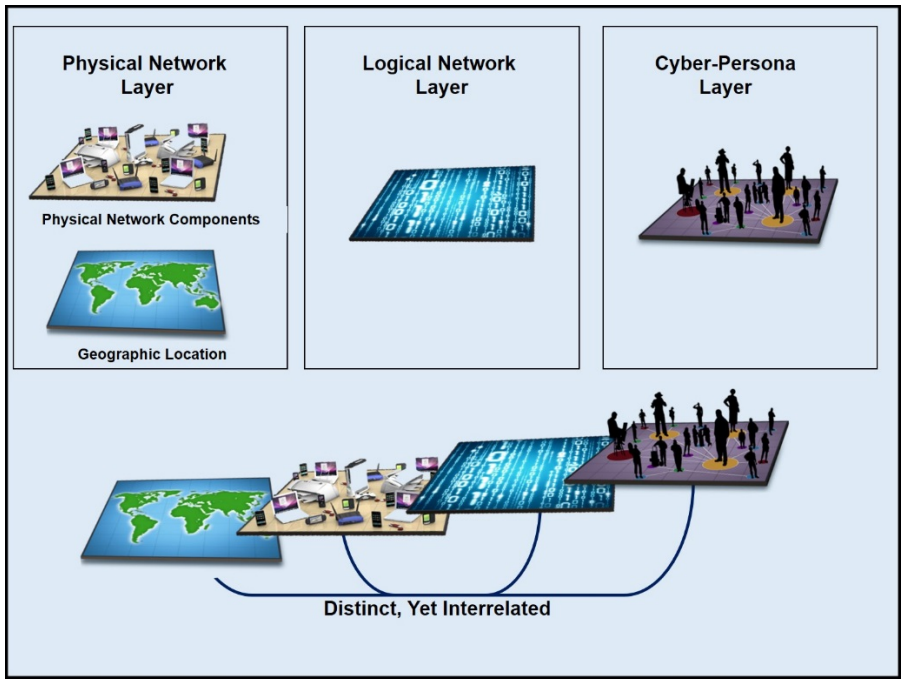

Figure 2-2. The Three Layers of Cyberspace[32]

4. **Cyberspace Location and Ownership**. Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations.

a. **Blue Cyberspace** denotes areas in cyberspace protected by the United States, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare, on order, and when requested by other authorities, to defend or secure other USG or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the United States and Partner Nations (PNs).

b. **Red Cyberspace** refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others.

c. **Gray Cyberspace**. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.[33]

5. **DOD Cyberspace**. The DODIN is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. The DODIN comprises all of DOD cyberspace, including the classified and unclassified global networks (e.g., NIPRNET, SIPRNET, Joint Worldwide Intelligence Communications System) and many other components, including DOD-owned smartphones, radio frequency identification tags, industrial control systems, isolated laboratory

networks, and platform information technology (PIT). PIT is the hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, including weapon systems. Nearly every military and civilian employee of DOD uses the DODIN to accomplish some portion of their mission or duties.[34]

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

1. Defining the problem is essential to addressing 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 the relevant actors and identifying the relationships and interactions among their respective desired conditions and objectives. The problem statement articulates how the operational variables can be expected to resist or facilitate transformation and how inertia in the OE can be leveraged to ensure the desired conditions are achieved.[35] The commander faces a unique set of cyberspace threats and challenges while directing CO in a complex global security environment.

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

a. **Nation State Threat**. This threat is potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to other actors. Some nations may employ cyberspace capabilities to attack or conduct espionage against the United States. Nation-state threats involve traditional adversaries; enemies; and potentially, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.

b. **Non-State Threats**. Non-state threats are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs), and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct direct terrorist actions within cyberspace. Criminal organizations may be national or transnational in nature and steal information for their own use, including selling it to raise capital and target financial institutions for fraud and theft of funds. They may also be used as surrogates by nation-states or non-state threats to conduct attacks or espionage through cyberspace.

c. **Individual Actors or Small Group Threat**. Even individuals or small groups of people can attack or exploit U.S. cyberspace, enabled by affordable and readily available techniques and malware. Their intentions are as varied as the number of groups and individuals. These threats exploit vulnerabilities to gain access to discover additional vulnerabilities or sensitive data or maneuver to achieve other objectives. Ethical hackers may share the vulnerability information with the network owners, but, more frequently, these accesses are used for malicious intent. Some threats are politically motivated and use cyberspace to spread their message. The activities of these small-scale threats can be co-opted by more sophisticated threats, such as criminal organizations or nation-states, often without their knowledge, to execute operations against targets while concealing the identity of the threat/sponsor and also creating plausible deniability.

d. **Accidents or Natural Hazards**. The physical infrastructure of cyberspace is routinely disrupted by operator errors, industrial accidents, and natural disasters. These

unpredictable events can have greater impact on joint operations than the actions of enemies. Recovery from accidents and hazardous incidents can be complicated by the requirement for significant coordination external to DOD and/or the temporary reliance on back-up systems with which operators may not be proficient.[36]

3. **Challenges**. In addition to 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**. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable. This effort requires significant analysis and, often, collaboration with non-cyberspace agencies or organizations. The ability to hide the sponsor and/or the threat behind a particular malicious effect in cyberspace makes it difficult to determine how, when, and where to respond. The design of the Internet lends itself to anonymity and, combined with applications intended to hide the identity of users, attribution will continue to be a challenge for the foreseeable future.

b. **Geography Challenges**. In cyberspace, there is no stateless maneuver space. Therefore, when U.S. military forces maneuver in foreign cyberspace, mission and policy requirements may require they maneuver clandestinely without the knowledge of the state where the infrastructure is located. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external operations in red and gray cyberspace, as well as internal protection effects in blue cyberspace.

c. **Technology Challenges**. Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. Cyberspace capabilities without hardware components can be replicated for little or no cost. This means that once discovered, these capabilities will be widely available to adversaries, in some cases before security measures in the DODIN can be updated to account for the new threat. In addition, since similar technologies around the world share similar vulnerabilities, a single adversary may be able to exploit multiple targets at once using the same malware or exploitation tactic. Malware can be modified (or be designed to automatically modify itself), complicating efforts to detect and eradicate it.[37]

4. **Cyber Operations against the United States (since 2010)**. In February 2018, the Director of National Intelligence (DNI) stated that, "The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected – with relatively little built-in security – and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyber attacks – such as data deletion or localized and temporary disruptions of critical infrastructure – against the United States in a crisis short of war." The assessment concluded that "Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Non-state actors will continue to use cyber operations for financial crime and to enable propaganda and messaging. The use of cyber attacks as a foreign policy tool outside of

military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and U.S. partners."[38] The following list includes cyberspace operations against the United States that have been acknowledged by the U.S. Government:

a. **Russia**. The DNI assessment stated that "We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine. The Russian Government is likely to build on the wide range of operations it is already conducting, including disruption of Ukrainian energy distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe U.S. and allied critical infrastructures, as well as target the United States, North Atlantic Treaty Organization (NATO), and allies for insights into U.S. policy."[39]

2015 – The DNI noted that Russian cyber actors were developing the 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.[40]

2016 – The Department of Justice (DOJ) announced that a grand jury returned an indictment charging 12 Russian nationals for committing federal crimes that were intended to interfere with the 2016 U.S. presidential election. All twelve defendants are members of the GRU, a Russian Federation intelligence agency within the Main Intelligence Directorate of the Russian military.[41]

2017 – In his testimony to the Senate Committee on Armed Services, Admiral Rogers, Commander USCYBERCOM, reported that the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS) issued an alert in July 2017 to public utilities concerning a new malware that targeted electrical grids in Ukraine the previous winter. He also added that the most costly cyber-attack in history, NotPetya, was launched by the Russian military in June 2017. NotPetya encrypted and essentially ruined hard drives on thousands of Ukrainian computers. This cyber attack quickly spread well beyond Ukraine, causing billions of dollars in damages to businesses across Europe and as far away as the United States.[42]

b. **China**. The DNI assessed that China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities. The Intelligence Community (IC) and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral U.S.-China cyber commitments of September 2015. Most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.[43]

2012 – 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.[44]

2013 – 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 were 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.[45]

2014 – A 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.[46]

2017 – Admiral Rogers testified that Presidents Obama and Xi committed in 2015 that our two countries would not conduct or knowingly support cyber-enabled theft of intellectual property for commercial gain. Subsequent evidence, however, suggests that hackers based in China sustained cyber espionage that exploited the business secrets and intellectual property of American businesses, universities, and defense industries. In the fall of 2017, the Justice Department unsealed indictments against three Chinese nationals, alleging they exfiltrated more than 400GB of data from several companies in the United States. In addition, the Chinese government could exploit the production of information and technology products to harvest corporate, government, and even personal data from foreign countries.[47]

c. **Iran**. The DNI stated that, Iran will continue working to penetrate U.S. and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries – especially Saudi Arabia and Israel. Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran’s recent restraint from conducting cyber attacks on the United States or Western allies. Iran’s cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.[48]

2011 – 2013 – A group sponsored by Iran's Islamic Revolutionary Guard Corps conducted a coordinated campaign of distributed denial of service (DDOS) attacks against 46 major companies, primarily in the U.S. financial sector. 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.[49]

2013 – 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.[50]

2014 – 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.[51] Iranian

actors also conducted a data deletion attack against the network of a U.S.-based casino.[52]

2017 – Although not directed against the United States, Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.[53]

d. **North Korea**. The DNI stated that we expect North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States. Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including DDOS attacks, data deletion, and deployment of ransomware.[54] Admiral Rogers added that, we do not see North Korean cyber actors having the technical competence or imperative to avoid uncontrolled damage if they conduct cyber attacks against private-sector targets, especially critical infrastructure.[55]

2014 – 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 Federal Bureau of Investigation (FBI).[56]

2016 – North Korean actors conducted the cyber theft of $81 million from the Bank of Bangladesh which had an indirect effect on U.S. financial markets**.**[57]

2017 – North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure.[58]

e. **Syria**.

2011 and 2013 – Two Syrian hackers were charged with targeting Internet sites – in the United States 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 used "spear-phishing" to collect 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.[59]

2014 – 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.[60]

2017 – A federal grand jury returned an 11-count indictment charging two Syrian men with offenses relating to their participation in a conspiracy to engage in computer hacking as members the SEA. According to allegations in the indictment, the conspirators focused on spear-phishing U.S. government, military, international organizations, and private-sector entities, including the Executive Office of the President, the U.S. Marine Corps, the National Aeronautics and Space Administration, National Public Radio, the Associated Press, Reuters, The Washington Post, The New York Times, CNN, The Onion, USA Today, The New York Post, Time, Human Rights Watch, and scores of other entities and individuals. The conspirators conducted spearfishing attacks to steal usernames and passwords which were used to deface websites, redirect

domains to sites controlled or utilized by the conspiracy, steal electronic mail, and hijack social media accounts.[61]

f. **Terrorists**. The DNI testified that terrorist groups will continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Given their current capabilities, cyber operations by terrorist groups mostly likely would result in personally identifiable information (PII) disclosures, website defacements, and denial-of-service attacks against poorly protected networks. Transnational criminals will continue to conduct for-profit cyber enabled crimes, such as theft and extortion against U.S. networks.[62]

2015 – The Islamic State in Iraq and Syria (ISIS) released sensitive information about U.S. military personnel, in an effort to inspire attacks.[63]

g. **Criminals**. The DNI stated that criminals are developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities. "Ransomware," malware that employs deception and encryption to block users from accessing their own data, has become a particularly popular tool of extortion. We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber-criminal tools as a relatively inexpensive and deniable means to enable their operations.[64]

2014 – 2016 – Four individuals, including two Russian Federal Security Service (FSB) officers, have been charged in connection with compromising at least 500 million Yahoo accounts.[65]

2016 – Criminals employed ransomware against the medical sector, disrupting patient care and undermining public confidence in some medical institutions.[66]

2017 – DOJ charged 36 individuals for their alleged roles in the Infraud Organization, an Internet-based cybercriminal enterprise engaged in the large-scale acquisition, sale, and dissemination of stolen identities, compromised debit and credit cards, personally identifiable information, financial and banking information, computer malware, and other contraband.[67]

h. **Insider Threats**.

2010 – 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 Significant Activity (SIGACT) reports (from Iraq and Afghanistan) from the Secret Internet Protocol Router Network (SIPRNET).[68]

2013 – Edward J. Snowden, was charged with violations of: Unauthorized Disclosure of National Defense Information; Unauthorized Disclosure of Classified Communication; and Theft of Government Property.[69]

2015 – A former U.S. Nuclear Regulatory Commission employee pleaded guilty to an 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.[70]

2017 – Reality Leigh Winner, a federal contractor from Augusta, GA, was charged with (and later pleaded guilty to) removing classified material from a government facility and mailing it to a news outlet.[71]

5. **Cyberspace Threat 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 user IDs 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)**. An 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.

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.[72]

i. **Ransomware**. A type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.[73]

j. **Sniffer**. A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they are also 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.

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

l. **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.

m. **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.[74]

VI. Cyberspace Assumptions.

1. Commanders and staff should review strategic guidance and direction to see if any assumptions are imposed on the planning process. Where there is insufficient information or guidance, the commander and staff identify assumptions to assist in framing solutions. At this stage, assumptions address strategic and operational gaps that enable the commander to develop the operational approach.[75]

2. **Characteristics of Cyberspace Capabilities**. While cyberspace is complex and ever changing, cyberspace capabilities, whether devices or computer programs, must reliably create the intended effects. However, cyberspace capabilities are developed based on environmental assumptions and expectations about the operating conditions that will be found in the OE. These conditions may be as simple as the type of computer operating system being used by an adversary or as complex as the exact serial number of the hardware or version of the software installed, what system resources are available, and what other applications are expected to be running (or not running) when the cyberspace capability activates on target. These expected conditions should be well documented by the capability developer and are important for planners and targeting personnel to understand as capability limitations. The extent to which the expected environmental conditions of a target cannot be confirmed through Intelligence, Surveillance and Reconnaissance (ISR) sources represents an increased level of risk associated with using the capability. All other factors being equal, cyberspace capabilities that have the fewest environmental dependencies and/or allow the operator to reconfigure the capability are preferred.[76]

VII. Cyberspace Actions and the Operational Approach.

1. The operational approach is a commander's description of the broad actions the force can take to achieve an objective in support of the national objective or attain a military end state. It is the commander's visualization of how the operation should transform current conditions into the desired conditions – the way the commander envisions the OE at the conclusion of operations to support national objectives. The operational approach is based largely on an understanding of the OE and the problem facing the commander.[77]

2. **Operations *'In'*, *'Through'*, and *'External'* to Cyberspace**. When developing an operational approach, commanders 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, sustainment, and information. These joint functions comprise related capabilities and activities grouped together to help commanders integrate, synchronize, and direct operations (see Figure 2-3).[78]

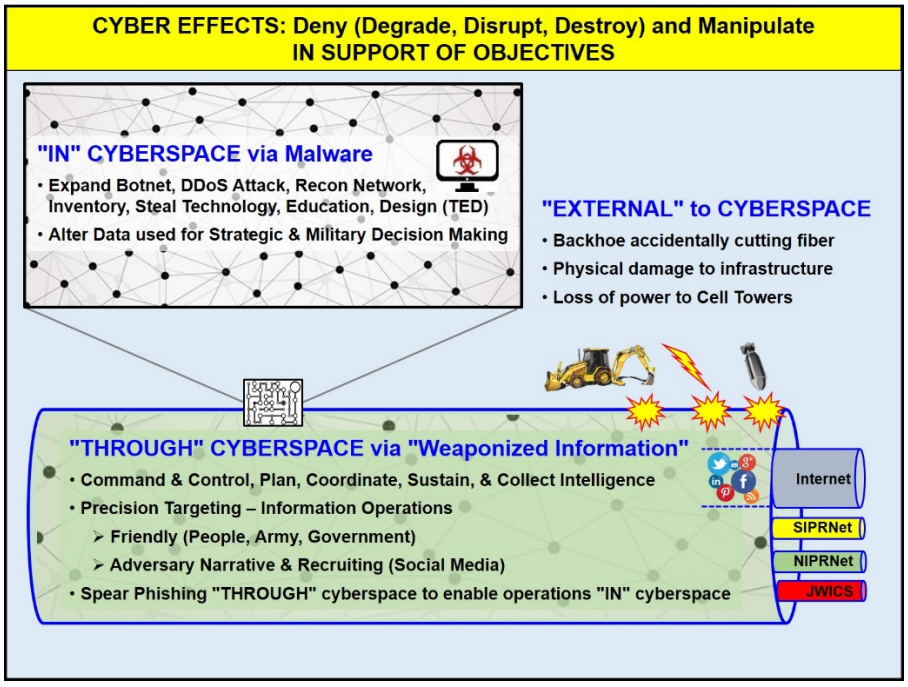

Figure 2-3: Operations In, Through, and External to Cyberspace

3. **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 United States 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.

4. **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 United States, is also a weakness that presents an opportunity to undermine U.S. capabilities in a very asymmetric way. The 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.[79]

5. **Cyberspace Missions**. All actions in cyberspace that are not simply cyberspace-enabled activities are taken as part of one of three cyberspace missions: DODIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO) (see Figure 2-4). Cyberspace Operations 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 integration and synchronization of these missions.

a. **DOD Information Network (DODIN) Operations**. The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN. These include proactive cyberspace security actions which address vulnerabilities of the DODIN or specific segments of the DODIN. DODIN operations are network-focused and threat-agnostic: the cyberspace forces and workforce undertaking this mission endeavor to keep all threats out of a particular network or system they are assigned to protect. DODIN operations is a standing mission, and although many DODIN operations activities are regularly scheduled events, they cannot be considered routine, since their aggregate effect establishes the framework on which most DOD missions ultimately depend.

b. **Defensive Cyberspace Operations (DCO)**. DCO missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace. Specifically, they are missions intended to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. This distinguishes DCO missions, which defeat specific threats that have bypassed, breached, or are threatening to breach security measures, from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any specific threat activity. DCO are threat-specific and frequently support mission assurance objectives. DCO missions are conducted in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity and leverage information from maneuver, intelligence collection, counterintelligence (CI), law enforcement (LE), and other sources as required. DCO include outmaneuvering or interdicting adversaries taking or about to take actions against defended cyberspace elements, or otherwise responding to imminent internal and external cyberspace threats. The goal of DCO is to defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state. The components of DCO are:

(1) **DCO Internal Defensive Measures (DCO-IDM)**. DCO-IDM are the form of DCO mission where authorized defense actions occur within the defended network or portion of cyberspace. DCO-IDM of the DODIN is authorized by

standing order and includes cyberspace defense actions to dynamically reconfirm or reestablish the security of degraded, compromised, or otherwise threatened DOD cyberspace to ensure sufficient access to enable military missions. For compromised DODIN elements, specific tactics include rerouting, reconstituting, restoring, or isolation. Most DCO missions are DCO-IDM, which include pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects.

(2) **DCO Response Actions (DCO-RA)**. DCO-RA are the form of DCO mission where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. DCO-RA actions are normally in foreign cyberspace. Some DCO-RA missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems, depending on broader operational context, such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat, the damage the threat has caused or is expected to cause, and national policy considerations. DCO-RA missions require a properly coordinated military order and careful consideration of scope, rules of engagement (ROE), and measurable objectives.

c. **Offensive Cyberspace Operations (OCO)**. OCO are CO missions intended to project power in and through foreign cyberspace through actions taken in support of Combatant Commander (CCDR) or national objectives. OCO may exclusively target adversary cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, etc. All CO missions conducted outside of blue cyberspace with a commander's intent other than to defend blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions. Like DCO-RA missions, some OCO missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems. Specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities and national policy considerations. OCO missions require a properly coordinated military order and careful consideration of scope, ROE, and measurable objectives.[80]

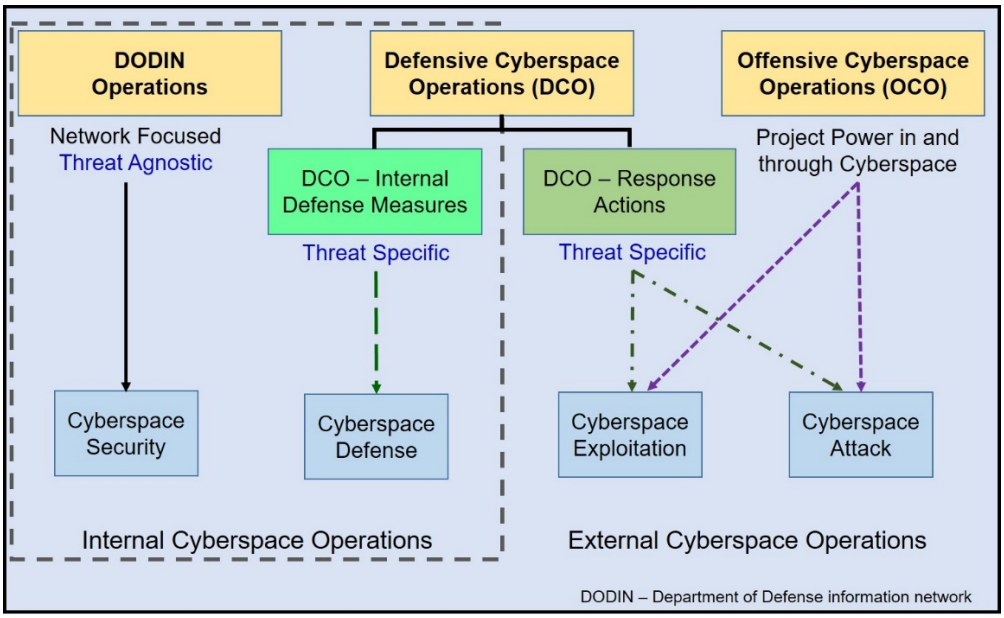

Figure 2-4: Cyberspace Missions and Actions[81]

6. **Cyberspace Actions**. Execution of any OCO, DCO, or DODIN operations mission requires completion of specific tactical-level actions or tasks that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of these actions, which are defined exclusively by the types of effects they create. To plan for, authorize, and assess these actions, it is important the commander and staff clearly understand which actions have been authorized under their current mission order. Since they will always be necessary, standing orders for DODIN operations and DCO-IDM missions cover most cyberspace security and initial cyberspace defense actions. However, OCO and DCO-RA missions are episodic. They may require clandestine maneuver and collection actions or may require overt actions, including fires. Therefore, the approval for CO actions in foreign cyberspace requires separate OCO or DCO-RA mission authorities. The cyberspace actions are:

a. **Cyberspace Security**. Cyberspace security actions are taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other IT, including PIT, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Although they are threat-informed, cyberspace security actions occur in advance of a specific security compromise and are a primary component action of the DODIN operations mission. Cyberspace security actions protect from threats within cyberspace by reducing or eliminating vulnerabilities that may be exploited by an adversary and/or implementing measures to detect malicious cyberspace activities.

b. **Cyberspace Defense**. Cyberspace defense actions are taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach the cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. The Combatant Command (CCMD), Service, or DOD agency that owns or operates the network is generally authorized to take these defensive actions except in cases when they would compromise the

operations of elements of cyberspace outside the responsibility of the respective CCMD, Service, or agency.

c. **Cyberspace Exploitation**. Cyberspace exploitation actions include military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation actions are taken as part of an OCO or DCO-RA mission and include all actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation also supports current and future operations through collection of information, including mapping red and gray cyberspace to support situational awareness; discovering vulnerabilities; enabling target development; and supporting the planning, execution, and assessment of military operations. Cyberspace exploitation actions are deconflicted with other USG departments and agencies in accordance with national policy.

d. **Cyberspace Attack**. Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains. Unlike cyberspace exploitation actions, which are often intended to remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality. Cyberspace attack actions are a form of fires, are taken as part of an OCO or DCO-RA mission, are coordinated with other USG departments and agencies, and are carefully synchronized with planned fires in the physical domains. They include actions to:

(1) **Deny**. To prevent access to, operation of, or availability of a target function by a specified level for a specified time, by:

- **Degrade**. To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified.
- **Disrupt**. To completely but temporarily deny 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 is 100 percent.
- **Destroy**. To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.

(2) **Manipulate**. Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. It uses an adversary's information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace. The targeted network may appear to

operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect.[82]

VIII. Identifying Cyberspace Decisions and Decision Points.

1. During planning, commanders inform leadership of the decisions that will need to be made, when they will have to be made, and the uncertainty and risk accompanying decisions and delay. This provides leaders, both military and civilian, a template and warning for the decisions in advance and provides them the opportunity to look across interagency partners and with allies to look for alternatives and opportunities short of escalation. The decision matrix also identifies the expected indicators needed in support of the intelligence collection plan.[83]

2. **Interagency Considerations**. When appropriate, commanders coordinate and integrate their CO with interagency partners during planning and execution. Effective integration of interagency considerations is vital to successful military operations, especially when the joint force conducts shaping, stability, and transition to civil authority activities.

3. **Multinational Considerations**. Commanders must consider the potential use of U.S. cyberspace forces to protect multinational force networks. Commanders should also anticipate and incorporate mission partner planning factors, such as their domestic laws, regulations, and operational limitations on the use of various cyberspace capabilities and tactics.[84]

IX. Refining the Cyberspace Operational Approach.

1. Throughout the planning processes, commanders and their staffs conduct formal and informal discussions at all levels of the chain of command. These discussions help refine assumptions, limitations, and decision points that could affect the operational approach and ensure the plan remains feasible, acceptable, and adequate. The commander adjusts the operational approach based on feedback from the formal and informal discussions at all levels of command and other information.[85]

2. **Intelligence Gain/Loss (IGL)**. Maneuver and fires in red and gray cyberspace could potentially compromise intelligence collection activities sources and methods. To the maximum extent practicable, an IGL assessment is required prior to executing such actions. The IGL assessment can be complicated by the array of non-DOD USG and multinational partners operating in cyberspace. Commanders use IGL analysis to weigh the risks of conducting the CO versus achieving the desired objective via other methods.[86]

3. **Targeting**. Although targets paired with cyberspace capabilities can often be engaged with no permanent damage, due to the interconnectedness of cyberspace, the effects of CO may cross geographical boundaries and, if not carefully planned, may have unanticipated effects. As a result, engaging targets in and through cyberspace requires close coordination within DOD and with interagency and multinational partners.[87]

4. **Risk Concerns**. Commanders should continuously seek to minimize risks to the joint force, as well as to friendly and neutral nations, societies, and economies, caused by use of cyberspace. Coordinated joint force operations benefit from the use of various cyberspace capabilities, including unclassified Web sites and Web applications used for communication efforts with audiences internal and external to DOD.[88]

X. Developing Cyberspace Planning Guidance.

1. The commander provides a summary of the OE and the problem, along with a visualization of the operational approach, to the staff and to other partners through commander's planning guidance. As time permits, the commander may be able to apply operational design to think through the campaign or operation before the staff begins JPP. In this case, the commander

provides initial planning guidance to help focus the staff in mission analysis. Commanders should continue the analysis to further understand and visualize the OE as the staff conducts mission analysis. Upon completing analysis of the OE, the commander will issue planning guidance, as appropriate, to help focus the staff efforts.[89]

2. Commanders integrate CO into their operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-critical cyberspace, access key terrain in cyberspace, operate in a degraded environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities. The commander provides initial planning guidance, which may specify time constraints, outline initial coordination requirements, authorize the movement of forces within the commander's authority, and direct other actions as necessary. Supporting CO plans and concepts describe the role and scope of CO in the commander's effort and address how CO support the execution of the supported plan. If requested by a commander, CDRUSCYBERCOM provides assistance in integrating cyberspace forces and capabilities into the commander's plans and orders.[90]

Intentionally Blank

Chapter 3: Planning

I. Joint Planning Process (JPP)

1. **Planning**. Plans translate the strategy into operations with the expectation that successful operations achieve the desired strategic objectives. Similarly, the effects of operations, successful or otherwise, change the operational and strategic environment, requiring constant evaluation of the strategic-level objectives to ensure they are still relevant and feasible. Joint forces, through their assessments, identify when their actions begin to negatively affect the Operational Environment (OE), and change their operations and activities to ensure better alignment between the actions and objectives.[91]

2. **Operational Design**. Operational design and JPP are complementary tools of the overall planning process. The commander, supported by the staff, gains an understanding of the OE, defines the problem, and develops an operational approach for the campaign or operation through the application of operational design during the initiation step of JPP.[92]

3. **JPP**. JPP is an orderly, analytical set of logical steps to frame a problem; examine a mission; develop, analyze, and compare alternative courses of action (COAs); select the best COA; and produce a plan or order. The application of operational design provides the conceptual basis for structuring campaigns and operations. JPP 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. It focuses on defining the military mission and development and synchronization of detailed plans to accomplish that mission (see Figure 3-1).[93]

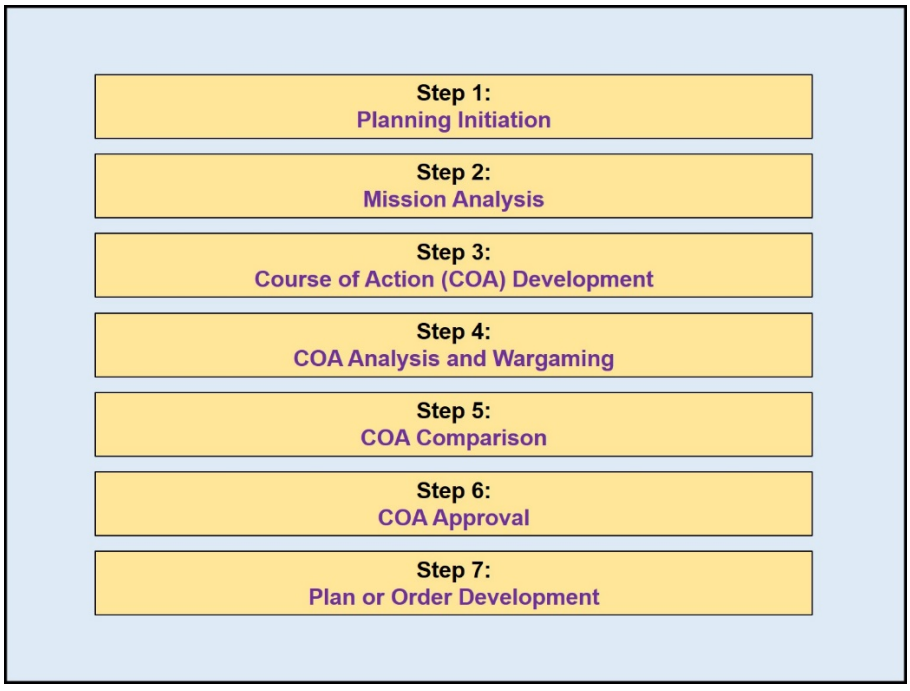

Figure 3-1: Joint Planning Process[94]

II. Cyberspace Operations Planning

1. **Planning Integration**. Commanders integrate cyberspace operations (CO) into their operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-critical cyberspace, access key terrain in cyberspace, operate in a degraded environment, efficiently

use limited cyberspace assets, and pair operational requirements with cyberspace capabilities. The commander provides initial planning guidance, which may specify time constraints, outline initial coordination requirements, authorize the movement of forces within the commander's authority, and direct other actions as necessary. Supporting CO plans and concepts describe the role and scope of CO in the commander's effort and address how CO support the execution of the supported plan.

2. **Planning Considerations**. Although CO planners are presented the same operational design considerations and challenges as planners for operations in the physical domains, there are some unique considerations for planning CO. For instance, because of unforeseen linkages in cyberspace, higher-order effects of some CO may be more difficult to predict. This may require more branch and sequel planning. Further, while many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors. For planning internal operations within Department of Defense (DOD) cyberspace, DOD Information Network (DODIN) operations and Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) planners require a clear understanding of which friendly forces or capabilities might be targeted by an adversary; what DODIN vulnerabilities are most likely to be targeted and the potential effects of the adversary's action; the mission assurance risks involved; and an understanding of applicable domestic, foreign, and international laws and U.S. Government (USG) policy. Threats in cyberspace may be nation-states, non-state groups, or individuals, and the parts of cyberspace they control are not necessarily within the geographic borders associated with the threat's nationality or proportional to their geopolitical influence. A criminal element, a politically motivated group, or even a well-resourced individual may have a greater presence and capability in cyberspace than do many nations. Moreover, many adversaries operate cyberspace capabilities from portions of cyberspace geographically associated with the United States or owned by a U.S. entity. Each of these factors complicates the planning of CO.

3. **Planning Timelines.** For external missions, it is essential Offensive Cyberspace Operations (OCO) and DCO Response Actions (DCO-RA) planners understand the authorities required to execute the specific CO actions proposed. The applicable authorities may vary depending upon the phase of the operation. This includes accounting for the lead time required to obtain the necessary intelligence to define the correct target; develop target access; confirm the appropriate authorities; complete necessary coordination, including interagency coordination and/or synchronization; and to verify the cyberspace capability matches the intended target using the results of technical assurance evaluations. For internal missions, the timelines for DCO-IDM and DODIN operations planners are impacted by other factors, including levels of automation available to manage network posture, availability of security solutions from commercial providers and their licensing requirements, and operational considerations that may impact a defender's abilities to maneuver or take systems off-line to better manage their protection. However, the planning fundamentals remain the same, and despite the additional considerations and challenges of integrating CO, planners use most elements of the traditional processes to implement the commander's intent and guidance.[95]

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

> a. **Planning Initiation (Step 1)**. Joint planning begins when an appropriate authority recognizes potential for military capability to be employed in support of national objectives or in response to a potential or actual crisis. At the strategic level, that authority – the President, Secretary of Defense (SecDef), or Chairman of the Joint

Chiefs of Staff (CJCS) – initiates planning by deciding to develop military options. Commanders also initiate planning on their own authority when they identify a planning requirement not directed by higher authority.[96]

(1) Cyberspace planners will initiate coordination with higher headquarters staff counterparts to obtain information on current and future CO, running estimates, and other CO planning products.

(2) Key Outputs:

- Updated cyberspace effects running estimate.[97]

b. **Mission Analysis (Step 2)**. The commander and staff analyzes the strategic direction and derives the restated mission statement for the commander's approval, which allows subordinate and supporting commanders to begin their own estimates and planning efforts for higher headquarters' concurrence. The joint force's mission is the task or set of tasks, together with the purpose, that clearly indicates the action to be taken and the reason for doing so. Mission analysis is used to study the assigned tasks and to identify all other tasks necessary to accomplish the mission.[98]

(1) Cyberspace planners gather, analyze, and synthesize information on current conditions of the operational environment with an emphasis on the cyberspace and information environment. The planners will coordinate with the intelligence staff to identify enemy and adversary capabilities and their use of cyberspace to assist in the development of models, situation templates, event templates, high-value targets, named areas of interest, and other outputs from the intelligence process, which include enemy and adversary cyberspace information.

(2) Key Outputs:

- List of cyberspace information requirements.
- Intelligence products to support CO.
- Most likely and most dangerous enemy COAs.
- CO specified and implied tasks.
- Cyberspace limitations and constraints.
- Cyberspace assumptions.
- Updated CO running estimate.[99]

c. **Course of Action (COA) Development (Step 3)**. A COA is a potential way (solution, method) to accomplish the assigned mission. The staff develops COAs to provide unique options to the commander, all oriented on accomplishing the military end state. A good COA accomplishes the mission within the commander's guidance, provides flexibility to meet unforeseen events during execution, and positions the joint force for future operations. It also gives components the maximum latitude for initiative. Planners can vary COAs by adjusting the use of joint force capabilities throughout the OE by employing the capabilities in combination for effectiveness making use of the information environment (including cyberspace) and the electromagnetic spectrum.[100]

(1) Cyberspace planners develop an initial CO scheme consisting of cyberspace support tasks that describes how the commander intends to use CO to support the concept of operations with an emphasis on the scheme of maneuver.

(2) Key Outputs:

- Updated CO information requirements.
- Initial high-payoff target list.
- Draft CO scheme including objectives and effects.
- Updated cyberspace operations running estimate.[101]

d. **COA Analysis, Wargaming, Comparison, and Approval (Steps 4, 5, and 6)**. 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 identify the advantages and disadvantages of each proposed friendly COA. The commander and staff analyze each COA separately according to the commander's guidance. Wargaming is a primary means to conduct this analysis. Once COA analysis is complete, the staff 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 objective is to identify and recommend the COA that has the highest probability of accomplishing the mission. Finally, the staff briefs the commander on the COA analysis, wargaming, and comparison results and the commander combines personal analysis with the staff recommendation to approve a COA.[102]

(1) Cyberspace planners refine their CO scheme, ensuring that it nests with the scheme of maneuver. Planners will provide recommendations for consideration during the COA comparison process. The best COA must first be ethical, and then the most effective and efficient possible. The commander will issue final planning guidance including refined commander's intent, commander's critical information requirements, and any additional guidance on priorities.

(2) Key Outputs

- Refined cyberspace input to commander's critical information requirements.
- Refined CO input to the high-payoff targets list.
- Refined CO scheme.
- Updated cyberspace effects and running estimate.
- Recommended course of action.
- Updated cyberspace effects running estimate.
- Commander approved COA.[103]

e. **Plan or Order Development (Step 7).** 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 plan or Operations Order (OPORD) by refining the initial Concept of Operations (CONOPS) associated with the approved COA. 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.[104]

(1) All planning products are finalized including the CO running estimate and Cyber Effects Request Format (CERF). As time permits, the staff may conduct a more detailed war game of the selected COA.[105]

5. **Intelligence Support to Cyberspace Operations Planning**. 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 COAs.[106]

a. **Understanding the OE** is fundamental to all joint operations, including CO. Intelligence may be derived from information gained during military operations in cyberspace or from other sources. All-source intelligence support to CO utilizes the same intelligence process used by all other military operations, with unique attributes necessary for support of CO planning. The process includes:

(1) Planning and direction, to include identification of target vulnerabilities to enable continuous planning and direction of counterintelligence (CI) activities to protect against espionage, sabotage, and attacks against U.S. citizens/facilities and continuously examining mission success criteria and associated metrics to assess the impact of CO and inform the commander's decisions.

(2) Collection sensors with access to information about cyberspace.

(3) Processing and exploitation of collected data, including identification of useful information from collected data, either real-time or after-the-fact.

(4) Analysis of information and production of intelligence products.

(5) Dissemination and integration of intelligence related to cyberspace with operations.

(6) Evaluation and feedback regarding intelligence effectiveness and quality.[107]

b. **Intelligence Requirements (IRs)**. During mission analysis, the joint force staff identifies significant information gaps about the adversary and other relevant aspects of the OE. After gap analysis, the staff formulates IRs, which are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based upon identified IRs, the 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 can include such things as network infrastructures and status, readiness of adversary's equipment and personnel, and unique cyberspace signature identifiers such as hardware/software/firmware versions and configuration files. These IRs are met through a combination of military intelligence and national intelligence sources.[108]

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 attacking 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 interagency (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 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.[109]

7. **Cyberspace Planning Support**. The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of malicious activity. The timing of planned CO should be determined based on a realistic assessment of their ability to create effects and support operations throughout the OE. This may require use of cyberspace capabilities in earlier phases of an operation than the use of other types of capabilities. Effective planners and operators understand how other operations within the OE may impact the CO.[110]

III. 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 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 3-2):[111]

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

(U) **References:** *Add any specific references to cyberspace 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 cyberspace; cyberspace may expand the area of local interest to a worldwide interest.*

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

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

d. (U) Friendly Forces. *Outline the higher headquarters' cyberspace activities 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 the subordinate commander. Identify friendly forces cyberspace vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the EMS, especially for joint or multinational operations. Deconflict and prioritize 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 3-2: Notional Cyberspace Operations Appendix
Adapted from FM 3-12, Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) to Operations Plans and Orders[112]

3. (U) **Execution**.

a. (U) Scheme of Cyberspace Electromagnetic Activities. *Describe how cyberspace and Electronic Warfare (EW) operations support the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how cyberspace and EW effects will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive cyberspace and EW measures. Identify target sets and effects, by priority. Describe the general concept for the integration of cyberspace and EW operations. List the staff sections, elements, and working groups responsible for aspects of cyberspace and electromagnetic activities. Include the cyberspace and EW collection methods for information developed in staff section, elements, and working groups outside the cyberspace operations support staff. 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 the components of cyberspace and EW and how these activities are integrated across the operational plan. It is recommended that this appendix include an understanding of technical requirements.*

This appendix concentrates on the integration requirements for cyberspace operations and references appropriate annexes and appendixes as needed to reduce duplication.

(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 and constraints. Identify risks associated with cyberspace operations. Include collateral damage, discovery, attribution, fratricide (to U.S. or allied or multinational networks or information), and possible conflicts. Describe actions that will prevent enemy and 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 warnings, and how they will be monitored. State how the cyberspace operations tasks will destroy, degrade, disrupt, and deny enemy computer networks. Identify and prioritize target sets and effect(s) in cyberspace. If appropriate, state how cyberspace operations support the accomplishment of the operation. Identify plans to detect or assign attribution of enemy and adversary actions in the physical domains and cyberspace. Ensure subordinate units are conducting defensive cyberspace operations (DCO). Synchronize the Cyber Electromagnetic Activities (CEMA) section with the IO officer. Pass requests for offensive cyberspace operations (OCO) to higher headquarters for approval and implementation. Describe how DOD information network operations support the commander's intent and concept of operations. Synchronize DODIN operations with the J-6. Prioritize the allocation of applications utilizing cyberspace. Ensure the employment of cyberspace 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 appendixes as needed to reduce duplication).*

(1) (U) DODIN Operations. *Describe how information 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.*

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

Figure 3-2 (Continued): Notional Cyberspace Operations Appendix

(3) (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 OCO.*

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 3-2 (Continued): Notional Cyberspace Operations Appendix

IV. Cyber Effects Request Format (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 and planners continue to develop and refine desired effects throughout JPP. Monitoring progress toward creating desired effects and avoiding undesired effects continues throughout execution.[113]

a. Commanders use CO to create effects in and through cyberspace in support of military objectives.[114] Although it is possible for CO to produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate most CO with other operations to create coordinated and synchronized effects required to support mission accomplishment.

b. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains. Actions in cyberspace, through carefully controlled cascading effects, can enable freedom of action for activities in the physical domains. Likewise, activities in the physical domains can create effects in and through cyberspace by affecting the electromagnetic spectrum (EMS) or the physical infrastructure.[115]

c. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external operations in red and gray cyberspace, as well as internal protection effects in blue cyberspace. The cumulative effects of some CO may extend beyond the initial target, a joint operations area (JOA), or outside of a single area of responsibility (AOR). Because of transregional considerations and the requirement for high-demand forces and capabilities, some CO are coordinated, integrated, and synchronized using centralized execution from a location remote from the supported commander.[116]

d. Cascading effects sometimes travel through systems subordinate to the one targeted but can also move laterally to peer systems or up to higher-level systems. Compounding effects are an aggregation of various levels of effects that have interacted in ways that may be intended or may have been unforeseen. Collateral effects, including collateral damage, are the incidental effects of military operations on non-combatants and civilian property that were not the intended targets of the strike. Depending upon the strategic and operational situation, an order or applicable rules of engagement (ROE) may limit CO to only those actions likely to result in no or low levels of collateral effects.[117]

2**. Cyber Effects Request**. Planning and targeting staffs develop and select targets in and through cyberspace based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and objectives, not on using a particular cyberspace capability simply because it is available.[118] The CERF is the format forces use to request effects in and through cyberspace (see Figure 3-3). As effects are determined for target and critical network nodes, the staff will prepare, submit, and track the CERF. This request will be integrated into the joint targeting cycle for follow on processing and approval. The joint task force (JTF), CCMD, and USCYBERCOM staff play a key role in processing the CERF and coordinating follow on cyberspace capabilities.[119]

CYBER EFFECTS REQUEST FORMAT (CERF)

SECTION 1: REQUESTING UNIT INFORMATION

Supported Major Command: _____

Date / Time Sent: _____

Requesting Unit: _____

Supported OPLAN/CONPLAN/ORDER: _____

Supported Mission Statement: _____

Supported Commander's Intent: _____

Supported Commander's End State: _____

Supported Concept of Operation: _____

Supported Objective (Strategic/Operational/Tactical): _____

Supported Tactical Objective/Task: _____

SECTION 2: CYBERSPACE OPERATIONS SPECIFIC INFORMATION

Type of Target (Scheduled / On Call): _____

Target Priority (Emergency / Priority / Routine): _____

Target Name: _____

Target Locator: _____

Target Description: _____

Desired Effect: _____

Target Function: _____

Target Significance: _____

TARGET DETAILS: *Include any relevant device information such as type, operating systems version and patch level, software, number of users, activity, friendly actors in the area of operations, surrounding / adjacent / parallel devices, etc.*

CONCEPT OF CYBER OPERATION: *Include Task, Purpose, Method, and End State. Also specify intelligence collection plan for battle damage assessment, to include allocated resources, measures of performance (MOPs), measures of effectiveness (MOEs), and MOE indicators.*

TARGET EXPECTATION STATEMENT: _____

REMARKS: If any of the following information is available, provide

(1) Time on Target / Duration of Effect
(2) No Earlier Than / No Later Than Need time
(3) Trigger Event or Conditions of Execution
(4) Persistence Requirement (i.e., effect must persist through a restart of the target, trigger event)
(5) Command and Control Requirement (i.e., effect must be able to be turned on/off remotely))
(6) Self-Destruct / Auto Delete Requirement (i.e., effect must stop itself if C2 is lost after X amount of time)
(7) Level of Attribution Requirement (i.e., attributable to CONUS/USG, misattributed to USG, etc.)
(8) Level of Detectability Allowed (i.e., should not be detected by (a) administrator, (b) user, (c) forensic analyst, etc.)
(9) Level Co-optability Allowed (i.e., low, medium, high)
(10) Remote Monitoring Requirement (i.e., effect should be able to be monitored by (a) operator, (b) JOC, etc.)
(11) Infrastructure Requirement (i.e., effect should be launched from specific infrastructure / system / platform)
(12) Reversibility Requirement (i.e., effect should be reversible / not reversible)

Figure 3-3: Cyber Effects Request Format (CERF)[120]
Adapted from FM 3-12, Annex C

Intentionally Blank

Chapter 4: Execution

I. Execution

1. **Execute Order (EXORD)**. Execution begins when the President or Secretary of Defense (SecDef) authorizes the initiation of a military operation or other activity. An EXORD, or other authorizing directive, is issued by the Chairman of the Joint Chiefs of Staff (CJCS) at the direction of the President or SecDef to initiate or conduct the military operations.[121]

2. **Planning During Execution** Planning continues as execution begins, with an initial emphasis on producing the Operations Order (OPORD) if one does not yet exist. As the operation progresses, planning generally occurs in three distinct but overlapping timeframes: future plans, future operations, and current operations (see Figure 4-1).

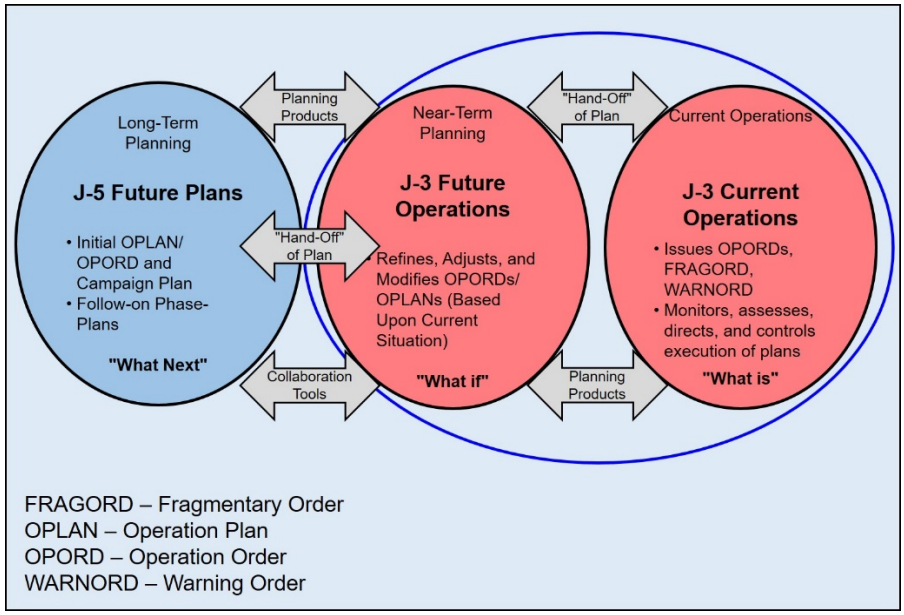

Figure 4-1: Planning During Execution[122]

a. 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's 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.

b. 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).

c. 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.

3. During execution, accomplishment of the plan’s tasks will be monitored and measured for how successfully each objective was completed, along with the input of new data and information as it is obtained to allow selection of branches or sequels, if applicable, or the plan

to be modified as necessary. Execution of a plan does not end the planning process. The staff may reenter the planning cycle 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.[123]

II. Cyberspace Operations During Execution.

1. **Execution**. Although cyberspace operations (CO) planners are presented the same operational design considerations and challenges as planners for operations in the physical domains, there are some unique considerations for planning CO. For instance, because of unforeseen linkages in cyberspace, higher-order effects of some CO may be more difficult to predict. This may require more branch and sequel planning. Further, while many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors. For planning internal operations within Department of Defense (DOD) cyberspace, DOD Information Network (DODIN) operations and Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) planners require a clear understanding of which friendly forces or capabilities might be targeted by an adversary; what DODIN vulnerabilities are most likely to be targeted and the potential effects of the adversary's action; the mission assurance risks involved; and an understanding of applicable domestic, foreign, and international laws and United States Government (USG) policy. Threats in cyberspace may be nation-states, non-state groups, or individuals, and the parts of cyberspace they control are not necessarily within the geographic borders associated with the threat's nationality or proportional to their geopolitical influence. A criminal element, a politically motivated group, or even a well-resourced individual may have a greater presence and capability in cyberspace than do many nations. Moreover, many adversaries operate cyberspace capabilities from portions of cyberspace geographically associated with the United States or owned by a U.S. entity. Each of these factors complicates the planning of CO.[124]

2. **Legal Considerations**. DOD conducts CO consistent with U.S. domestic law, applicable international law, and relevant USG and DOD policies. Therefore, DOD cyberspace forces that operate outside the DODIN, when properly authorized, are generally limited to operating in gray and red cyberspace only, unless they are issued different rules of engagement (ROE) or conducting Defense Support of Civil Authorities (DSCA) under appropriate authority. Since each CO mission has unique legal considerations, the applicable legal framework depends on the nature of the activities to be conducted, such as Offensive Cyberspace Operations (OCO) or DCO, DSCA, Intelligence, Surveillance, and Reconnaissance (ISR) actions, Law Enforcement (LE) and Counterintelligence (CI) activities, intelligence activities, and defense of the homeland. Before conducting CO, commanders, planners, and operators require clear understanding of the relevant legal framework to comply with laws and policies, the application of which may be challenging given the global nature of cyberspace and the geographic orientation of domestic and international law. It is essential commanders, planners, and operators consult with legal counsel during planning and execution of CO (see Appendix A: DOD Law of War Manual excerpt).[125]

3. **Cyberspace Authorities.** Authorities for specific types of military CO are established within SecDef policies, including DOD instructions, directives, and memoranda, as well as in EXORDs and OPORDs authorized by the President or SecDef and subordinate orders issued by commanders approved to execute the subject missions. These include the directive authority for cyberspace operations (DACO), established by CJCS EXORD, that enables DOD-wide synchronized protection of the DODIN (see Figure 4-2).

US Code (USC)	Title	Key Focus	Principle Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18 Title 28	*Crimes and Criminal Procedure* *Judiciary and Judicial 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 44	*Public Printing and Documents*	Defines basic agency responsibilities and authorities for information security policy	All Federal departments and agencies	The foundation for what we now call cybersecurity activities, as outlined in Department of Defense Instruction, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations*
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the DOD 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 4-2: United States Code-Based Authorities[126]

4. **Command and Control of Cyberspace Forces**. Clearly established command relationships are crucial for ensuring timely and effective employment of forces, and CO require unity of command and unity of effort. However, the complex nature of CO, where cyberspace forces can be simultaneously providing actions at the global level and at the theater or Joint Operations Area (JOA) level, requires adaptations to traditional command and control (C2) structures. The CJCS has established two models for C2 of CO, depending upon the prevailing circumstances – normal operating conditions and when a cyberspace-related crisis or contingency is in effect (see Figure 4-3).

a. **C2 for Global CO**. CDRUSCYBERCOM is the supported commander for transregional and global CO and manages day-to-day global CO even while he or she is the supporting commander for one or more geographic or functional Combatant Commander's (CCDR's) operations. A supported relationship for CO does not exempt either command from coordinating response options with affected commanders prior to conducting an operation. JFHQ-DODIN centrally coordinates and directs global DODIN operations and DCO-IDM when these operations have the potential to impact the integrity and operational readiness of multiple DOD components. Although execution of many actions may be decentralized, CDRUSCYBERCOM is the supported commander for CO to secure, operate, and defend the DODIN and, when ordered, to defend other U.S. critical cyberspace assets, systems, and functions.

b. **C2 for CO Supporting CCMDs**. CCDRs are supported for CO in their area of responsibility (AOR) or for their transregional responsibilities, with CDRUSCYBERCOM supporting as necessary. These CO comprise actions intended to have effects localized within a Geographic Combatant Commander's (GCC's) AOR or a Functional Combatant Commander's (FCC's) transregional responsibilities. These could be cyberspace

security and defense actions internal to a theater DODIN segment or external actions, such as cyberspace exploitation or cyberspace attack against a specific enemy capability. In addition to the theater segments of global networks, CCMD-level DODIN operations and DCO-IDM include the protection of stand-alone and tactical networks and computers used exclusively by the CCMD. For example, CCMD-level maneuvers in cyberspace include activities to reposition capabilities to enhance threat detection in specified areas, focus cyberspace forces activity in areas linked to specific operational branches and sequels to keep the adversary at risk, or activate stand-by tactical cyberspace capabilities to transition friendly C2 to more secure locations. Such CO maneuvers are vital when a CCDR's systems are under attack to the degree that subsets of the DODIN are degraded, compromised, or lost. In such operations, the supported CCDR coordinates, through their USCYBERCOM CO-Integrated Planning Element (CO-IPE), with their associated enterprise operation center, supported by JFHQ-DODIN and Defense Information Systems Agency (DISA), to restore the affected cyberspace. The supported CCDR also integrates, synchronizes, and normally directs CO actions in red and gray cyberspace, including fires, with other lethal and nonlethal effects, for which they may use assigned, attached, or supporting cyberspace forces. CCDRs develop and coordinate their requirements for such effects with the USCYBERCOM CO-IPE, for deconfliction and prioritized execution. When a CCDR establishes a subordinate force (e.g., a joint task force), the cyberspace unit(s) assigned to support that force are determined by the CCDR's mission requirements in coordination with CDRUSCYBERCOM.

5. **Cyberspace Organizations and Forces**. CCMDs Integrate cyberspace capabilities into military operations and work closely with the joint force, USCYBERCOM, Service Cyberspace Components (SCCs), and DOD agencies to create fully integrated capabilities. (Appendix B provides an overview of U.S. cyberspace organizations).[127]

a. **Combatant Command (CCMD) Cyberspace Operations Support Staffs**. CCDRs size and structure their CO support staff to best support their mission and requirements. This staff, supported by a USCYBERCOM CO-IPE, coordinates CO requirements and capabilities throughout their planning, intelligence, operations, assessment, and readiness processes to integrate and synchronize CO with other military operations. Additionally, as necessary and in partnership with USCYBERCOM, the CCMD coordinates regionally with interagency and multinational partners. The CCMD:

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

(2) Facilitates, through USCYBERCOM, coordination and deconfliction of CCDR-directed CO which may impact or conflict with other DOD or other USG cyberspace activities or operations within the AOR. As early as possible in the planning process, provide USCYBERCOM with sufficient information about CCDR-planned CO to enable deconfliction with other USG CO.

b. **USCYBERCOM Cyberspace Operations – Integrated Planning Element (CO-IPE)**. USCYBERCOM CO-IPEs are organized to meet individual CCMD requirements and facilitate planning and coordination of all three cyberspace missions, as required. USCYBERCOM CO-IPEs remain in direct support of and are integrated with CCMD CO staff to provide a bridge for USCYBERCOM and its subordinate Headquarters (HQ) to enable theater/tactical and global/national integration of cyberspace forces and operations.[128]

c. **Mission Tailored Force Package (MTFP)**. A MTFP is a USCYBERCOM-tailored support capability comprised of assigned CO forces, additional CO support personnel, and cyberspace capabilities, as required. When directed, USCYBERCOM establishes a tailored force to support specific CCMD crisis or contingency mission requirements beyond the capacity of forces available for routine support. Each MTFP is task-organized and provided to the supported CCDR for the duration of the crisis/contingency operation or until redeployed by CDRUSCYBERCOM in coordination with the supported CCDR.[129]

d. **Joint Force Headquarters – Department of Defense Information Networks (JFHQ-DODIN)**. In coordination with all CCDRs and other DOD components, JFHQ-DODIN conducts the operational-level planning, direction, coordination, execution, and oversight of global DODIN operations and DCO-IDM missions. Maintains support relationships, as established by CDRUSCYBERCOM, with all CCDRs for theater/functional DODIN operations and DCO-IDM. Commander, JFHQ-DODIN, is supported for global DODIN operations and DCO-IDM, and CCDRs are supported for DODIN operations and DCO-IDM with effects contained within their AOR or functional mission area. JFHQ-DODIN exercises DACO over all DOD components as delegated by CDRUSCYBERCOM.[130]

e. **Cyber Mission Force (CMF)**. The focus of USCYBERCOM's Cyber Mission Force teams aligns with the DOD Cyber Strategy's three primary missions: Defend DOD networks and ensure their data is held secure; support joint military commander objectives; and, when directed, defend U.S. critical infrastructure. Specifically, Cyber Mission Force teams support these mission sets though their respective assignments:

(1) Cyber Protection Force (CPF) teams defend the DODIN and assigned cyberspace, protect priority missions, and prepare cyber forces for combat. The CPF comprises:

- Cyberspace Protection Teams (CPTs).

(2) Cyber National Mission Force (CNMF) teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them. The CNMF comprises:

- National Mission Teams (NMTs)
- National Support Teams (NSTs)

(3) Cyber Combat Mission Force (CCMF) teams conduct military cyber operations in support of combatant commands. The CCMF comprises:

- Combat Mission Teams (CMTs)
- Combat Support Teams (CSTs).

f. **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 CCMD 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 CCMD

cyberspace operations support staff 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.

(1) **JFHQ-C Marine Forces Cyber Command** supports U.S. Special Operations Command.

(2) **JFHQ-C Army Cyber Command** supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command.

(3) **JFHQ-C Fleet Cyber Command** supports U.S. Pacific Command and U.S. Southern Command.

(4) **JFHQ-C Air Force Cyber Command** supports U.S. European Command, USSTRATCOM, and U.S. Transportation Command.[131]

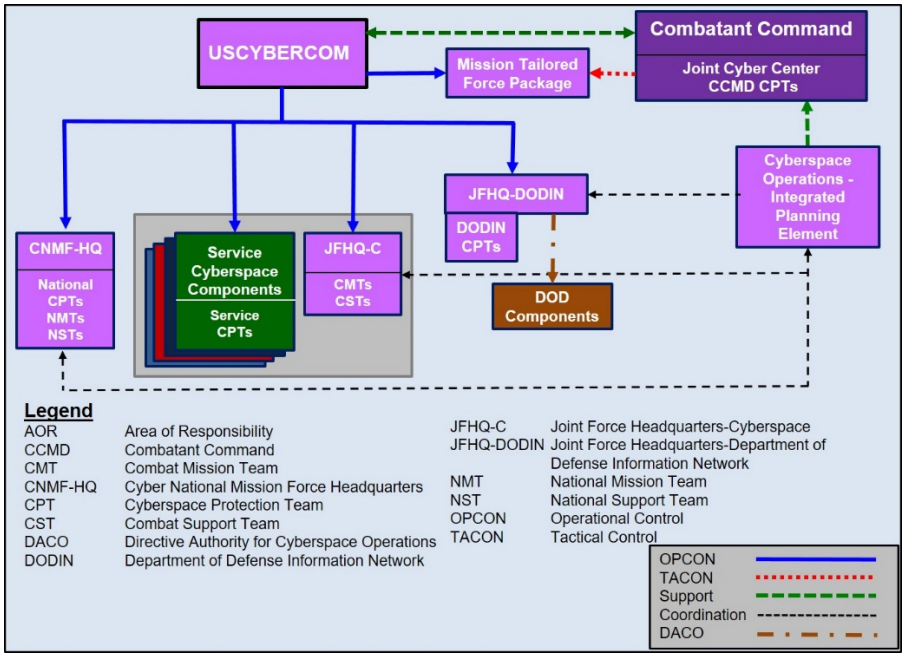

Figure 4-3: Crisis/Contingency Cyberspace Command and Control
Adapted From JP 3-12, Figure IV-4[132]

6. **Synchronization of Cyberspace Operations**. The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of malicious activity. CO deconfliction and coordination efforts in or through cyberspace should include similar measures:

a. **Deconfliction**. For CO, deconfliction is the act of coordinating the employment of cyberspace capabilities to create effects with applicable DOD, interagency, and multinational partners to ensure operations do not interfere, inhibit, or otherwise conflict with each other. The commander’s intended effects in cyberspace, and the capabilities planned to create these effects, require deconfliction with other commands and agencies that may have equities in the same area of cyberspace.

b. **Electromagnetic Spectrum (EMS) Factors** has significant implications for CO. The commander uses joint EMS operations to coordinate elements of CO, space operations, electronic warfare (EW), navigation warfare, various forms of EMS-dependent information collection, and C2. Although these activities can be integrated with other information-related capabilities (IRCs) as part of information operations synchronization, the offensive aspects of CO, space operations, and EW operations are often conducted under different specific authorities. Likewise, some IRCs enabled by CO, such as military information support operations (MISO) and military deception (MILDEC), have their own execution approval process. Therefore, synchronizing IRCs that use the EMS is a complex process that requires significant foresight and awareness of the various applicable policies.

c. **Integration of Cyberspace Fires**. Cyberspace attack capabilities, although they can be used in a stand-alone context, are generally most effective when integrated with other fires. Some examples of integrating cyberspace fires are: disruption of enemy air defense systems using EMS-enabled cyberspace attack, insertion of messages into enemy leadership's communications, degradation/disruption of enemy space-based and ground-based precision navigation and timing systems, and disruption of enemy C2. Effects in cyberspace can be created at the strategic, operational, or tactical level, in any phase of the military operation, and coordinated with lethal fires to create maximum effect on target. Integrated fires are not necessarily simultaneous fires, since the timing of cyberspace attack effects may be most advantageous when placed before or after the effects of lethal fires. Each engagement presents unique considerations, depending upon the level and nature of the enemy's dependencies upon cyberspace. Supporting cyberspace fires may be used in a minor role, or they can be a critical component of a mission when used to enable air, land, maritime, space, and special operations. Forces operating lethal weapons and other capabilities in the physical domains cannot use cyberspace fires to best advantage unless they clearly understand the type and timing of planned effects in cyberspace. Properly prepared and timed cyberspace fires can create effects that cannot be created any other way. Poorly timed fires in cyberspace can be useless, or even worse, interfere with an otherwise effective mission.[133]

7. **Cyberspace Targeting**. The purpose of targeting is to integrate and synchronize fires (the use of weapon systems or other actions to create a specific lethal or nonlethal effect on a target) into joint operations. The Review and Approval Process for certain OCO and DCO-RA missions is unique to CO and applies to many aspects of the joint targeting cycle. Therefore, CO planners and decision makers often use a targeting process specifically adapted to the circumstance.

a. **Cyberspace Targeting Process**. Planning and targeting staffs develop and select targets in and through cyberspace based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and objectives, not on using a particular cyberspace capability simply because it is available. Integrating and synchronizing planning, execution, and assessment are pivotal to the success of joint targeting. Three fundamental aspects of CO require consideration in the targeting processes:

(1) Recognizing cyberspace capabilities are a viable option for engaging some designated targets.

(2) Understanding a CO option may be preferable in some cases, because it may offer low probability of detection and/or no associated physical damage.

(3) Higher-order effects on targets in cyberspace may impact elements of the DODIN, including retaliation for attacks attributed to the joint force.

b. **Cyberspace Targeting Challenges**. Every target has distinct intrinsic or acquired characteristics (i.e., physical, functional, cognitive, environmental, and temporal) that form the basis for detection, location, and identification; for determining target value within the target system; and for classification for future surveillance, analysis, strike, and assessment. The challenge in targeting for CO is to identify, correlate, coordinate, and deconflict multiple activities occurring across the physical network, logical network, and cyberpersona layers. This requires a C2 capability that can operate at the tempo of CO and can rapidly integrate impacted stakeholders.

(1) The **physical network layer** is the medium where the data travels. It includes wired (e.g., land and undersea cable) and wireless (e.g., radio, radio-relay, cellular, satellite) transmission means. It is a point of reference for determining geographic location and the applicable legal framework.

(2) The **logical network layer** provides an alternate view of the target, abstracted from its physical location, and referenced from its logical position in cyberspace. This position is often represented through a network address (e.g., internet protocol [IP] address). It depicts how nodes in the physical domains address and refer to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical domains may be lost. Targeting in the logical layer requires the logical identity and logical access to the target to have a direct effect.

(3) The **cyber-persona layer**, the aggregate of an individual's or group's online identity(ies), and an abstraction of logical network layer data, holds important implications for joint forces in terms of positive target identification and affiliation and activity attribution. Cyber-personas are created to group information together about targeted actors in order to organize analysis, engagement, and intelligence reporting. Because cyber-personas can be complex, with elements in many virtual locations but often not linked to a single physical location or form, sufficient intelligence collection and analysis capabilities are required for the joint forces to gain insight and situational awareness required to enable effective targeting of a cyber-persona. Ultimately, cyber-personas will be linked to features that will be engaged in either the logical or physical network layers.

c. **Cyberspace Target Access**. Cyberspace forces develop access to targets or target elements in cyberspace by using cyberspace exploitation actions. This access can then be used for various purposes, ranging from information collection to maneuver and to targeting nomination. Not all accesses are equally useful for military operations. For instance, the level of access required to collect information from an entity may not be sufficient to create a desired effect. Developing access to targets in or through cyberspace follows a process which can often take significant time. In some cases, remote access is not possible, and close proximity may be required. All target access efforts in cyberspace require coordination with the Intelligence Community (IC) for deconfliction in accordance with national policy and to illuminate potential IGL concerns. If direct access to the target is unavailable or undesired, sometimes a similar or partial effect can be created by indirect access using a related target that has higher-order effects on the desired target. Some denial of service cyberspace attacks leverage this type of indirect access.

d. **Cyberspace Target Nomination and Synchronization**. CO use standard target nomination processes, but target folders should include unique cyberspace aspects (e.g., hardware and software configurations, IP address, cyber-persona applications) of

the target. Development of this data is imperative to understand and characterize how elements targetable through cyberspace are relevant to the commander's objective. This data also allows the planner to match an appropriate cyberspace capability against a particular target. Component commanders, national agencies, supporting commands, and/or the planning staff nominate targets to the targeting staff for development and inclusion on the joint target list (JTL). Once placed on the JTL, commanders in receipt of an EXORD with relevant objectives and ROE can engage the target with organic assets (if within a component commander's assigned area of operations) or nominate the target to CDRUSCYBERCOM for action by other joint force components and other organizations.

e. **Time-Sensitive Targets (TSTs)**. A TST is a validated target of such high priority to friendly forces that the commander designates it for immediate engagement because it poses (or will soon pose) a threat to friendly forces or is a highly lucrative, fleeting target. Engaging TSTs in cyberspace is difficult in most situations, because they are likely to cross-AORs and require detailed joint, interagency, and/or multinational planning efforts. Being prepared to engage a TST in cyberspace requires coordination between cyberspace planners, operators, and the supported commander early in the planning phase, to increase the likelihood that adequate flexibility and access is available should a fleeting opportunity arise.[134]

8. **Assessment of Cyberspace Operations**. Assessment measures progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of CO and compare them to their vision and intent. Measuring this progress toward the end state, and delivering timely, relevant, and reliable feedback into the planning process to adjust operations during execution, involves deliberately comparing the forecasted effects of CO with actual outcomes to determine the overall effectiveness of cyberspace force employment. The assessment process for external CO missions begins during planning and includes measures of performance (MOPs) and measures of effectiveness (MOEs) of fires and other effects in cyberspace, as well as their contribution to the larger operation or objective. Assessing the impact of CO effects requires typical BDA analysis and assessment of physical, functional, and target system components. However, the higher-order effects of cyberspace actions are often subtle, and assessment of second- and third-order effects can be difficult. Therefore, assessment of fires in and through cyberspace frequently requires significant intelligence collection and analysis efforts.[135]

Intentionally Blank

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[136]

I. Department of Defense Missions in the Homeland

1. **Strategy**. In support of the National Security Strategy, the Department of Defense (DOD) will be prepared to defend the homeland, remain the preeminent military power in the world, ensure the balances of power remain in our favor, and advance an international order that is most conducive to our security and prosperity.[137]

2. **Missions**. DOD is the lead federal agency (LFA) for defending against traditional external threats or aggression (e.g., nation-state conventional forces or weapons of mass destruction attack) and against external asymmetric threats that are outside of the scope of HS operations. The Department of Homeland Security (DHS) is the LFA for homeland security (HS), and the United States Coast Guard (USCG) is the LFA for maritime homeland security (MHS). By law, DOD is responsible for two missions in the homeland: homeland defense (HD) and defense support of civil authorities (DSCA). DOD also supports HS and may be required to participate in emergency preparedness (EP).

a. **Homeland Defense (HD)**. HD 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, DOD executes HD by detecting, deterring, preventing, and defeating threats from actors of concern as far forward from the homeland as possible. HD is executed across the active, layered defense construct composed of the forward regions, the approaches, and the homeland. Commander, U.S. Northern Command (CDRUSNORTHCOM), and Commander, U.S. Pacific Command (CDRUSPACOM), are the supported commanders for HD in their respective areas of responsibility (AORs), with all other combatant commanders (CCDRs) as supporting commanders.[138]

b. **Defense Support of Civil Authorities (DSCA)**. DSCA is support provided by U.S. federal military forces, DOD civilians, DOD contract personnel, DOD component assets, reserve and National Guard (NG) forces (when SecDef, in coordination with the governor[s] of the affected state[s], elect and request to use those forces under Title 32, United States Code [USC], Section 502) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement (LE) support, and other domestic activities or from qualifying entities for special events.

c. **Homeland Security (HS)**. DOD supports HS operations through DSCA and by providing DOD forces and capabilities to USCG MHS. HS is the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, LE, customs, border control, and immigration.

d. **Emergency Preparedness (EP)**. EP includes measures taken in advance of an emergency to reduce the loss of life and property and to protect a nation's institutions from all types of hazards through five preparedness mission areas under the National Response Framework (NRF). These five mission areas are prevention, protection, mitigation, response, and recovery.

3. **Interagency/Intergovernmental Coordination**. Within the homeland, HD, DSCA, and HS require pre-event and ongoing coordination with inter-organizational and multinational partners to integrate capabilities and facilitate unified action. In this complex environment, there are numerous threats across multiple jurisdictions (i.e., federal, state, local, and tribal) that are addressed by a diverse group of actively involved stakeholders (e.g., international organizations, multinational partnerships, nongovernmental organizations [NGOs], and the private sector). DOD plans and prepares to operate in concert with other U.S. Government (USG) entities. (see Figure 5-1).[139]

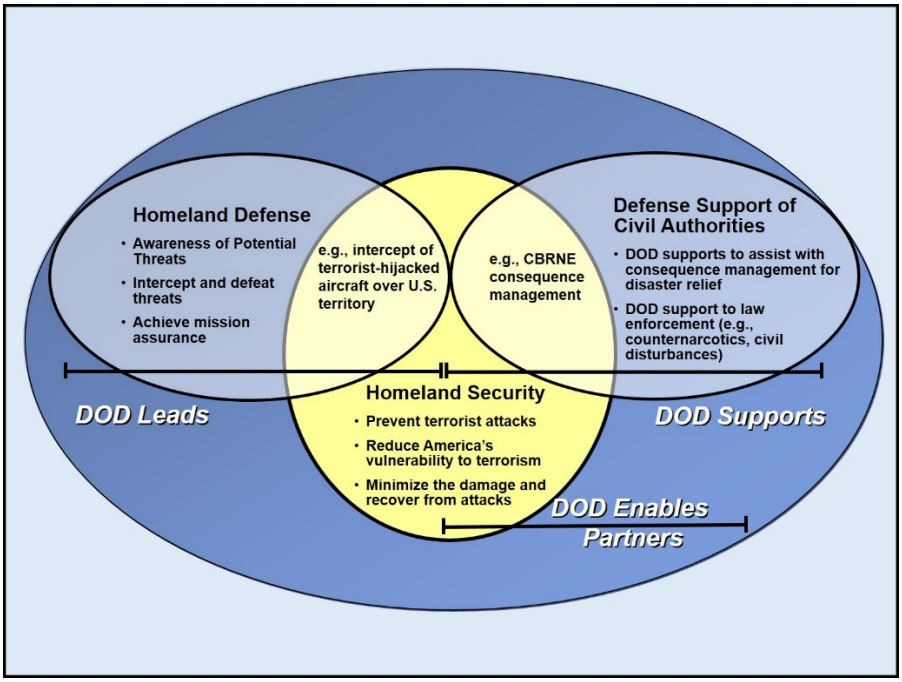

Figure 5-1: Active, Layered Defense of the United States

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. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered 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. Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors and designates responsibility to various Federal Government departments and agencies to serve as Sector-Specific Agencies (SSAs) for each of the critical infrastructure sectors:

a. **Chemical Sector** – Department of Homeland Security

b. **Commercial Facilities Sector** – Department of Homeland Security

c. **Communications Sector** – Department of Homeland Security

d. **Critical Manufacturing Sector** – Department of Homeland Security

e. **Dams Sector** – Department of Homeland Security

f. **Defense Industrial Base Sector** – Department of Defense

g. **Emergency Services Sector** – Department of Homeland Security

h. **Energy Sector** – Department of Energy

i. **Financial Services Sector** – Department of the Treasury

j. **Food and Agriculture Sector** – Department of Agriculture and Department of Health and Human Services

k. **Government Facilities Sector** – Department of Homeland Security and General Services Administration

l. **Healthcare and Public Health Sector** – Department of Health and Human Services

m. **Information Technology Sector** – Department of Homeland Security

n. **Nuclear Reactors, Materials, and Waste Sector** – Department of Homeland Security

o. **Transportation Systems Sector** – Department of Homeland Security and Department of Transportation

p. **Water and Wastewater Systems Sector** – Environmental Protection Agency[140]

III. Defense Critical Infrastructure Program

1. **DOD Responsibilities**. The DOD has two roles for critical infrastructure protection, first as a Federal department and second as a SSA for one of 16 national infrastructure sectors – the Defense Industrial Base. Within DOD, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, ASD (HD&ASA), 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&ASA) oversees the day-to-day execution of these 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 SSA 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.[141]

IV. Cyberspace Operations in the Conduct of Homeland Defense

1. **DOD Cyber Strategy**. The United States 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. DOD is focused on building the capabilities, processes, and plans necessary to succeed in this mission (see Figure 5-2).[142]

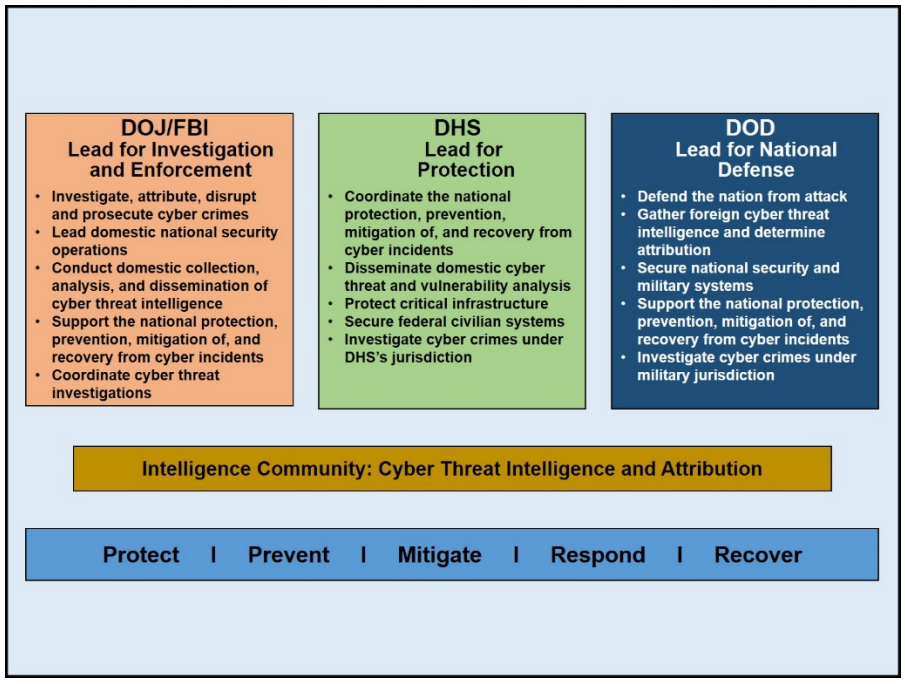

Figure 5-2: National Cybersecurity Roles and Responsibilities

2. **Unified Action**. For cyberspace, the vulnerability and complex interrelationship of national and international networks demand closely coordinated action among the military, private sector, and other government entities at all levels. Combatant Command (CCMD) cyberspace operations (CO) support staff, the Services, and U.S. Cyber Command (USCYBERCOM) are the military front line of defense. DHS has the responsibility for securing U.S. cyberspace at the

national level by protecting non-DOD USG networks against cyberspace intrusions and attacks. Within DHS, the Office of Cybersecurity and Communications (CS&C) is tasked to protect USG network systems from cyberspace threats. USPACOM and USNORTHCOM, because of their HD and DSCA responsibilities, have unique coordination requirements for CO through their CO support staff with USCYBERCOM.[143]

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 Chairman of the Joint Chiefs of Staff (CJCS) and CCMDs. USCYBERCOM also coordinates 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.[144]

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

a. **CDRUSNORTHCOM** is responsible for defending against, mitigating, and defeating cyberspace threats against USNORTHCOM and NORAD missions that are not associated with the defense of the DODIN in coordination with USCYBERCOM and USPACOM. USNORTHCOM will plan and execute CO during HD in coordination with USCYBERCOM. Finally, 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.[145]

b. **CDRUSPACOM** is responsible for defending against, mitigating, and defeating cyberspace threats against specific USPACOM systems that are not associated with the DODIN. HQ USPACOM will coordinate CO with USPACOM component commands, subordinate unified commands, joint task forces (JTFs), direct reporting units, and other CCMDs through USPACOM’s CO support staff; USCYBERCOM provides a cyberspace forward support element to USPACOM to support CO and as required for liaison between USCYBERCOM and USPACOM components. For HD, USPACOM coordinates through USCYBERCOM with DHS through its CS&C as the 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.[146]

4. **Cyberspace Operations Forces and Missions**. USCYBERCOM's second major mission objective is to defend the United States against cyber threats to U.S. interests and infrastructure. The command is concerned that many such cyber attacks now occur below the threshold of the use of force and outside of the context of armed conflict, but cumulatively accrue strategic gains to our adversaries.[147] Defending the nation in cyberspace is complex in both technical and policy terms. Like all Combatant Commands, USCYBERCOM is authorized only on order from the President (or the SecDef if the President is unavailable) to defend against a threat to the nation that would qualify as a "use of force" under international law.

a. The **Cyber National Mission Force (CNMF)** focuses on countering adversaries' malicious cyber activities against the United States and prepares to conduct full-spectrum cyberspace operations against adversaries when directed. The CNMF is building a force of National Mission Teams (NMTs), National Support Teams (NSTs), and National Cyber Protection Teams (N-CPTs). Partnering with NSA, the CNMF tracks adversary cyber actors to gain advantages that will enable the United States to preclude cyber-attacks against U.S. national interests. The CNMF is working with operational partners to develop and exercise the capabilities and operational concepts needed to enable combined and coalition operations (when authorized) in partnership with other government and appropriate private-sector partners.

b. **Whole of Nation Effort**. USCYBERCOM manages only a portion of the "whole-of-nation" effort required to defend America's critical infrastructure. The Command works with civilian agencies under their authorities to help protect national critical infrastructure and to prepare for scenarios in which U.S. military action to defend the nation may be required. The Department of Justice (DOJ) is the lead for cyber-related investigations and law enforcement, while the DHS takes the lead for national protection and recovery from cyber incidents. The Command is expanding its ties with the Reserves and the National Guard. Cyber response teams operating under Guard authorities can perform a variety of missions in support of state, local, and private entities (which operate independently under their own authorities). Recent legislation to incentivize information sharing will also help the Command and DOD to work more closely with the private sector in mitigating threats outside of government and military systems. The federal government has created a framework for implementing official channels to share information, and clarifying the lanes in the road for U.S. government assistance to the private sector.[148]

5. **Defense Industrial Base (DIB)**. DOD has the lead for improving security of the DIB sector, which includes major sector contractors and major contractor support to operations regardless of corporate country of domicile and continues to support the development of whole-of-government approaches for its risk management. The global technology supply chain affects mission-critical aspects of the DOD enterprise, and the resulting IT risks can only be effectively mitigated through public-private sector cooperation. DOD partners with the DIB to increase the security of information about DOD programs residing on or transiting DIB unclassified networks. The Department of Defense Cyber Crime Center (DC3) serves as DOD's operational focal point for voluntary cyberspace information sharing and incident reporting program. In addition, DOD is strengthening its acquisition regulations to require consideration of applicable cybersecurity policies during procurement of all DODIN components to reduce risks to joint operations.[149] DOD 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 DC3.

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.[150]

6. **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, DOD 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.[151] CI/KR consist of the infrastructure and assets vital to the nation's security, governance, public health and safety, economy, and public confidence. 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 DC3. Concurrent with its national defense and incident response missions, DOD may be directed to support DHS and other USG departments and agencies to help ensure all sectors of cyberspace CI/KR are available to support national objectives.

a. **Defense Critical Infrastructure (DCI)**. DCI is a subset of CI/KR that includes DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide. Geographic combatant commanders (GCCs) have the responsibility to prevent the loss or degradation of DCI within their AORs and coordinate with the DOD asset owner, heads of DOD components, and critical infrastructure sector lead agents to fulfill this responsibility. As the lead agent of the DODIN sector of the DCI, the Commander, Joint Force Headquarters-DODIN (JFHQ-DODIN), is responsible for matters pertaining to the identification, prioritization, and remediation of critical DODIN infrastructure issues. Likewise, DOD coordinates and integrates when necessary with DHS for support of efforts to protect the DIB.[152]

b. **DOD Reliance on Critical Infrastructure**. Many of DOD's critical functions and operations rely on contracted commercial assets, including Internet service providers (ISPs) and global supply chains, over which DOD and its forces have no direct authority. This includes both data storage services and applications provided from a cloud computing architecture. Cloud computing enables DOD to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. But, the overall success of these initiatives depends upon well-executed risk mitigation and protection measures, defined and understood by both DOD components and industry. Dependency on commercial Internet providers means DOD coordination with DHS, other interagency partners, and the private sector is essential to establish and maintain security of DOD's information. DOD supports DHS, which leads interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure.[153]

c. **Critical Infrastructure Owners' Responsibilities**. DOD 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.[154]

d. **DOD Exercise Program**. DOD's annual exercise program 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 CCMDs and combat support agencies can partner with DHS and FBI and other agencies to improve integration, training and support.[155] The CYBER GUARD operational-level command exercise validates operational concepts accounting for state governors' and National Guard Adjutant Generals' concerns about protecting critical assets. Both CYBER GUARD and CYBER FLAG exercises include players from the other CCMDs, as well as whole-of-government and industry participants to evaluate cyber capabilities in a DSCA scenario involving foreign intruders in the nation's critical infrastructure. USCYBERCOM has synchronized its efforts with the Chief of the National Guard Bureau in the CYBER SHIELD exercise as well as with DHS partners in the CYBER PRELUDE exercise.[156]

e. **DOD Policy**. DOD has established policies for cyber support to consult, coordinate, train, advise, and assist state and local agencies and domestic critical infrastructure as well as provide support to LE, HD, and DSCA activities in support of national objectives. [157]

(1) **Coordinate, Train, Advise, and Assist (CTAA)**. DOD Policy authorizes CTAA cyber support and services provided incidental to military training to organizations and activities and for National Guard personnel use of DOD information networks, software, and hardware for State cyberspace activities. DOD CTAA cyber support and services do NOT include:

- Offensive Cyberspace Operations or Defensive Cyberspace Operations – Response Actions.
- Support for civilian law enforcement purposes.

(2) **Consult**. Outside the context of CTAA training activities, DOD Components (including National Guard units serving in a title 32 U.S. Code, duty status) may consult with government entities and with public and private utilities, critical infrastructure owners, the DIB, and other non-governmental entities to protect DOD information networks, software, and hardware, enhance DOD cyber situational awareness, provide for DOD mission assurance requirements, and in order to provide cybersecurity unity of effort.[158]

(3) **Defense Support to Cyber Incident Response (DSCIR)**. DOD policy authorizes DSCIR within the framework of DSCA. DSCIR may include direct on-location support, remote support, or a combination of both as appropriate. DSCIR may be provided using DOD military, civilian, and contractor personnel (including National Guard units serving in a title 32 U.S. Code, duty status). Requests for assistance for DSCIR will be considered only if they include:

- Written acknowledgment that the entity receiving federal support understands that the federal support may include DOD support, which would be provided through the lead federal agency.

- Written permission for DOD to access appropriate information and information systems (e.g., applicable hardware, software, networks, servers, IP addresses, and databases).[159]

V. Department of Homeland Security Cyberspace Responsibilities

1. DHS has the responsibility to secure U.S. cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace intrusions and attacks, including actions to reduce and consolidate external access points, deploy passive network defenses and sensors, and define public and private partnerships in support of national cybersecurity policy.

2. DHS protects USG network systems from cyberspace threats and partners with government, industry, and academia, as well as the international community, to make cybersecurity a national priority and a shared responsibility.

3. Pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive-5, Management of Domestic Incidents, the Secretary of Homeland Security is the principal federal official for domestic incident management. Pursuant to PPD-41, *United States Cyber Incident Coordination*, DHS is the lead federal agency for cyberspace incident asset response. For significant cybersecurity incidents external to the DODIN and Intelligence Community (IC) networks, DHS's National Cybersecurity and Communications Integration Center is the lead federal agency for technical assistance and vulnerability mitigation.[160]

VI. Department of Justice (DOJ) Cyberspace Responsibilities

1. DOJ, including the FBI, leads counterterrorism and CI investigations and related LE activities associated with government and commercial CI/KR. DOJ investigates, defeats, prosecutes, and otherwise reduces foreign intelligence, terrorist, and other cyberspace threats to the nation's CI/KR. The FBI is the lead agency for significant cybersecurity incident threat response activities, except those that affect the DODIN or the IC. Given the ability of malicious cyberspace activity to spread, investigation of threats to the DODIN will need to be coordinated with the FBI.

2. The FBI also conducts domestic collection, analysis, and dissemination of cybersecurity threat information and operates the National Cyber Investigative Joint Task Force, a multi-agency focal point for coordinating, integrating, and sharing pertinent information related to cybersecurity threat investigations, with representation from DHS, the IC, DOD, and other agencies as appropriate.[161]

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[162]

a. **Multi-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 distributed denial-of-service (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 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 known 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 of that capacity 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.[163]

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.[164]

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 (CO) 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).

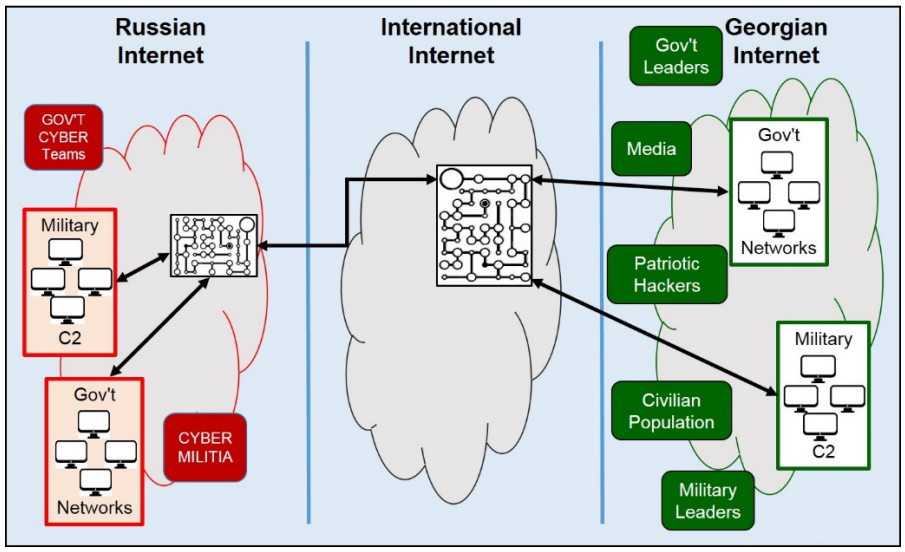

Figure 6-2: Georgian, Russian, and International Cyberspace Environment
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

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).

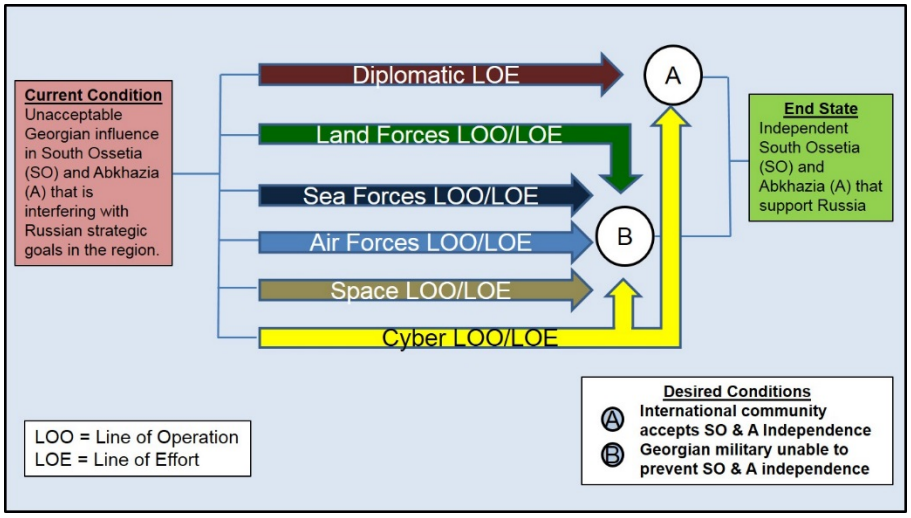

Figure 6-3: Russian Operational Approach in Georgia
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

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).

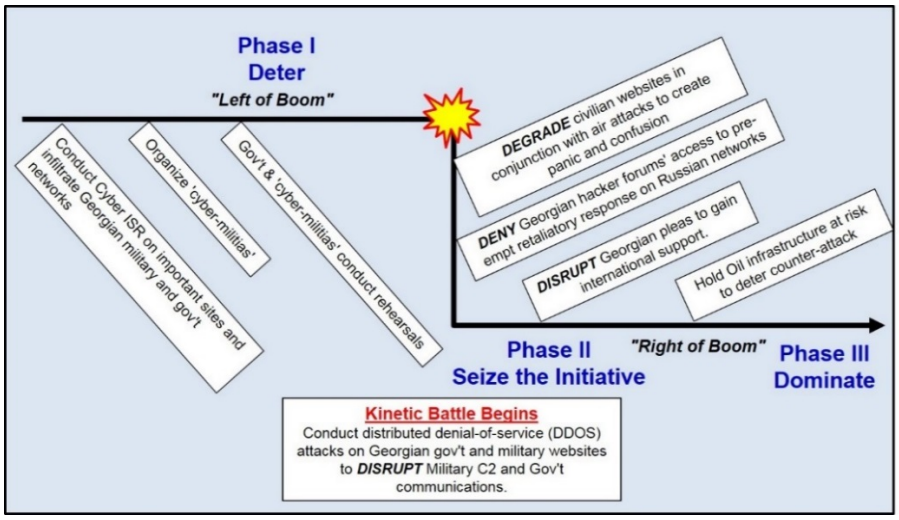

Figure 6-4: Russian Cyberspace Operations Concept in Georgia
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

4. **Cyberspace Operations during Execution**. Planning continues during execution, with an initial emphasis on refining the existing plan and producing the Operation Order (OPORD). 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).

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.

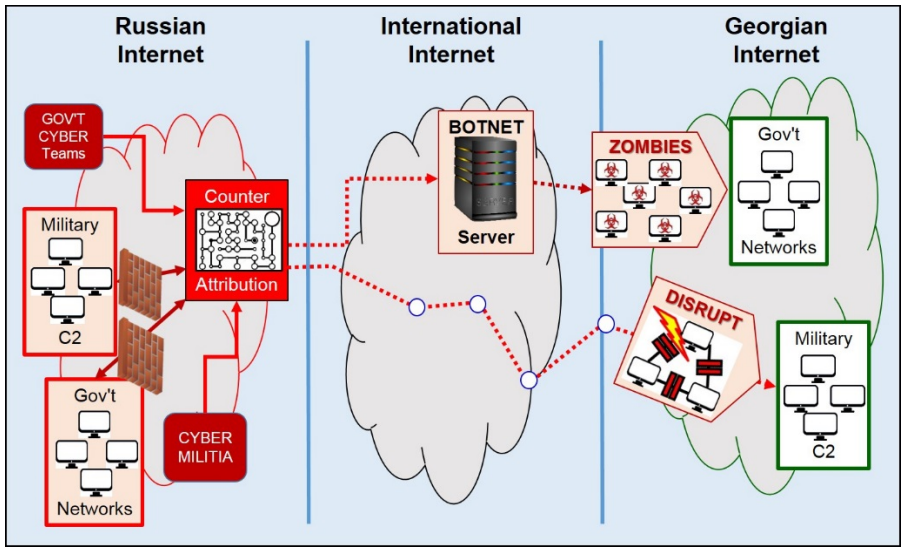

Figure 6-5: Russian Cyberspace Enabled Effects
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

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.[165] 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 CO teams attempted to conduct information network operations (similar to Department of Defense Information Network [DODIN] 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.[166]

b. **Defensive Cyberspace Operations (DCO)**. The Georgian CO teams conducted passive and active defensive 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.[167] 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.[168]

(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.[169]

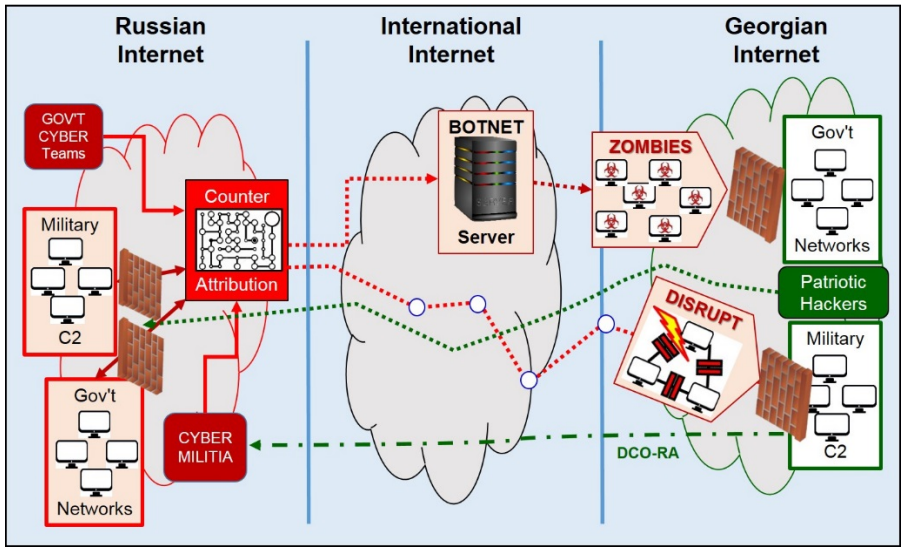

Figure 6-6: Georgian Defensive Cyberspace Operations (DCO)
(Original graphic derived from content of *Cross Domain Synergy in Joint Operations*)

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

Appendix A includes:

I. **U.S. Strategy and Policy**
   - **National Cyber Strategy of the United States of America**
   - **Department of State International Cyberspace Policy Strategy**
   - **Presidential Executive Order on Strengthening the Cybersecurity**
   - **Departmental Responses to Executive Order on Strengthening Cybersecurity**

II. **Department of Homeland Security Strategy and Guidance**
   - **The Cybersecurity Strategy for the Homeland Security Enterprise**
   - **Framework for Improving Critical Infrastructure Cybersecurity**

III. **Department of Justice Cyber Strategy and Guidance**
   - **DOJ 2018 Report of the Attorney General's Cyber-Digital Force**

IV. **Department of Defense Strategy**
   - **DOD Cyber Strategy**

V. **U.S. Cyber Law Guidance**
   - **DOS Position on International Law in Cyberspace**
   - **DOD Law of War Manual**

I. U.S. Strategy and Policy

A. National Cyber Strategy of the United States of America

President Trump released the National Cyber Strategy in September 2018. The introduction to the strategy is provided below, the full document can be found at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Introduction

America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge. Building on the National Security Strategy and the Administration's progress over its first 18 months, the National Cyber Strategy outlines how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity.

How Did We Get Here?

The rise of the Internet and the growing centrality of cyberspace to all facets of the modern world corresponded with the rise of the United States as the world's lone superpower. For the past quarter century, the ingenuity of the American people drove the evolution of cyberspace, and in turn, cyberspace has become fundamental to American wealth creation and innovation. Cyberspace is an inseparable component of America's financial, social, government, and political life. Meanwhile, Americans sometimes took for granted that the supremacy of the United States in the cyber domain would remain unchallenged, and that America's vision for an open, interoperable, reliable, and secure Internet would inevitably become a reality. Americans believed the growth of the Internet would carry the universal aspirations for free expression and individual liberty around the world. Americans assumed the opportunities to expand communication, commerce, and free exchange of ideas would be self-evident. Large parts of the world have embraced America's vision of a shared and open cyberspace for the mutual benefit of all.

Our competitors and adversaries, however, have taken an opposite approach. They benefit from the open Internet, while constricting and controlling their own people's access to it, and actively undermine the principles of an open Internet in international forums. They hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world. They view cyberspace as an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable.

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and inter-national businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors — including terrorists and criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states. Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities. Entities across the United States have faced cybersecurity

challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents.

The Way Forward

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive. Securing cyberspace is fundamental to our strategy and requires technical advancements and administrative efficiency across the Federal Government and the private sector. The Administration also recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront. The United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

The Administration is already taking action to aggressively address these threats and adjust to new realities. The United States has sanctioned malign cyber actors and indicted those that have committed cybercrimes. We have publicly attributed malicious activity to the responsible adversaries and released details of the tools and infrastructure they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing the cybersecurity risks to systems they control, while empowering them to provide adequate security.

The Administration's approach to cyberspace is anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy. We retain our commitment to the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies. The future we desire will not come without a renewed American commitment to advance our interests across cyberspace.

The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons.

This National Cyber Strategy outlines how we will:

> (1) defend the homeland by protecting networks, systems, functions, and data;
>
> (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
>
> (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and
>
> (4) expand American influence a broad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive,

disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives.

The articulation of the National Cyber Strategy is organized according to the pillars of the National Security Strategy. The National Security Council staff will coordinate with departments, agencies, and the Office of Management and Budget (OMB) on an appropriate resource plan to implement this Strategy. Departments and agencies will execute their missions informed by the following strategic guidance.

Source: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed 1 November 2018.

B. Department of State International Cyberspace Policy Strategy

The following is an excerpt of testimony by Christopher Painter, Department of State (DOS) Coordinator for Cyber Issues, before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, on 25 May 2016: https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

In May 2016, as required by the Consolidated Appropriations Act for 2016, the Department submitted to Congress the Department of State International Cyberspace Policy Strategy (the Strategy) that included a report on the Department's work to implement the President's 2011 *International Strategy for Cyberspace*, as well as a discussion of our efforts to promote norms of responsible state behavior in cyberspace, alternative concepts for norms promoted by certain other countries, threats facing the United States, tools available to the President to deter malicious actors, and resources required to build international norms.

In spite of the successes outlined in the Strategy, the U.S. vision for an open, interoperable, secure, and reliable Internet faces a range of policy and technical challenges. Many of these challenges were described in my testimony last year, and they largely remain. I would like to focus my time today delving specifically into our efforts to promote a broad international framework for cyber stability, as well some of the alternative views regarding the Internet that some governments are promoting. I will also spend some time discussing the technical challenges and threats posed by continuing malicious cyber activity directed at the United States, as well as our allies, and the tools we have at our disposal to deter these actions.

Diplomatic Efforts to Shape the Policy Environment

Building a Framework for International Stability in Cyberspace

The Department of State, working with our interagency partners, is guided by the vision of the President's International Strategy for Cyberspace, which is to promote a strategic framework of international cyber stability designed to achieve and maintain a peaceful cyberspace environment where all states are able to fully realize its benefits, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for states to engage in disruptive behavior or to attack one another.

This framework has three key elements: (1) global affirmation that international law applies to state behavior in cyberspace; (2) development of an international consensus on and promotion of additional voluntary norms of responsible state behavior in cyberspace that apply during peacetime; and (3) development and implementation of practical confidence building measures (CBMs), which promote stability in cyberspace by reducing the risks of misperception and escalation.

Since 2009, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has served as a productive and groundbreaking expert-level venue for the United States to build support for this framework. The consensus recommendations of the three UN GGE reports in 2010, 2013, and 2015 have set the standard for the international community on international cyberspace norms and CBMs. The UN GGE process will continue to play a central role in our efforts to fully promulgate this framework when it reconvenes in August 2016.

Applicability of international law. The first and most fundamental pillar of our framework for international cyber stability is the applicability of existing international law to state behavior in cyberspace. The 2013 UN GGE report was a landmark achievement that affirmed the applicability of existing international law, including the UN Charter, to state conduct in cyberspace. The 2013 report underscored that states must act in cyberspace under the

established international obligations and commitments that have guided their actions for decades – in peacetime and during conflict – and states must meet their international obligations regarding internationally wrongful acts attributable to them. The 2014-2015 UN GGE also made progress on issues related to international law by affirming the applicability of the inherent right to self-defense as recognized in Article 51 of the UN Charter, and noting the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction.

Norms of responsible state behavior. The United States is also building consensus on a set of additional, voluntary norms of responsible state behavior in cyberspace that define key areas of risk that would be of national and/or economic security concern to all states and which should be off-limits during times of peace. If observed, these stability measures – which are measures of self-restraint – can contribute substantially to conflict prevention and stability. The United States was the first state to propose a set of specific peacetime cyber norms, including the cybersecurity of critical infrastructure, the protection of computer security incident response teams (CSIRTs), and cooperation between states in responding to appropriate requests in mitigating malicious cyber activity emanating from their territory. In May 2015, Secretary of State Kerry highlighted these norms in his speech in Seoul, South Korea, on an open and secure Internet. The 2015 UN GGE report's most significant achievement was its recommendation for voluntary norms of state behavior designed for peacetime, which included concepts championed by the United States.

Confidence Building Measures. Together with our work on law and voluntary norms, cyber CBMs have the potential to contribute substantially to international cyber stability. CBMs have been used for decades to build confidence, reduce risk, and increase transparency in other areas of international concern. Examples of cyber CBMs include: transparency measures, such as sharing national strategies or doctrine; cooperative measures, such as an initiative to combat a particular cyber incident or threat actor; and stability measures, such as committing to refrain from a certain activity of concern. Cyber CBMs are being developed, and are in the first stages of implementation, in two regional venues – the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum where agreement was reached in 2015 on a detailed work plan with a proposed set of CBMs for future implementation.

Although many of the elements of the framework I have described above may seem self-evident to an American audience, it is important to recognize that cyber issues are new to many states, and as I describe later in my testimony, there are also many states that hold alternative views on how we should promote cyber stability. Notwithstanding these headwinds, as well as the fact that diplomatic negotiations on other issues can take many years, if not decades, the United States and its allies have made substantial progress in recent years towards advancing our strategic framework of international cyber stability. At this point, I would like to highlight examples from last year that reflect our progress.

U.S.-China Cyber Commitments

The United States strongly opposes the use of cyber technology to steal intellectual property for commercial advantage, and has raised this concern with Chinese interlocutors for several years. In 2014, the United States indicted five members of the Chinese military for hacking, economic espionage, and other offenses directed at six U.S. entities. This led China to suspend the U.S.-China Cyber Working Group. The United States and China, however, reached agreement during President Xi Jinping's state visit in September 2015 on several key commitments on cyber issues. These commitments are:

(1) both governments agreed to cooperate and provide timely responses to requests for information and assistance regarding malicious cyber activity emanating from their territories;

(2) neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property for commercial advantage;

(3) both governments will work together to further identify and promote appropriate norms of state behavior in cyberspace and hold a senior experts group on international security issues in cyberspace; and

(4) both governments will establish a Ministerial-level joint dialogue mechanism on fighting cybercrime and related issues.

On 11 May 2016, the United States hosted the first meeting of the senior experts group in Washington on international security issues in cyberspace, which provided a forum to further engage China on its views and seek common ground regarding norms of state behavior in cyberspace and other topics. The Department of State led the U.S. delegation that included participation from the Department of Defense and other U.S. government agencies. The senior experts group helps us advance the growing international consensus on international law and voluntary cyber norms of state behavior. We also have encouraged China to join us in pushing for other states to affirm these principles in international forums like the Group of Twenty (G20), and will continue to do so.

To implement other commitments reached during President Xi's visit, the United States and China held the first ministerial level dialogue on cybercrime and other related issues in Washington on December 1, 2015. Attorney General Loretta Lynch and Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor Guo Shengkun, co-chaired the first U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues to foster mutual understanding and enhance cooperation on law enforcement and network protection issues. The second dialogue is scheduled to occur next month in Beijing, China.

Moreover, regarding the commitment that neither government will conduct or knowingly support cyber-enabled theft for commercial gain, Deputy Secretary of State Blinken testified last month before the full Committee on Foreign Relations that the United States is "watching very closely to ensure this commitment is followed by action."

The outcomes of last year's Xi-Obama summit focus on concrete actions and arrangements that will allow us to hold Beijing accountable to the commitments they have made. These commitments do not resolve all our challenges with China on cyber issues. However, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship.

Group of Twenty (G20) Antalya Summit

In November 2015, the leaders of the G20 met in Antalya, Turkey, to discuss and make progress on a wide range of critical issues facing the global economy. At the conclusion of the Antalya Summit, the strong final communique issued by the G20 leaders affirmed the U.S.-championed vision of international cyber stability and its pillars.

Among other things, the G20 leaders affirmed in their statement that "no country should conduct or support the [Information and Communication Technologies] ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." They also highlighted the "key role played by the United Nations in developing norms" and the work of the UN GGE and its 2015 report. Addressing our overall framework, the G20 leaders stated that they "affirm

that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behavior in the use of ICTs… ."

The G20 leaders' communique represents a remarkable endorsement of our approach to promoting stability in cyberspace. But there is still more to do. The United States will continue to work within the G20 and in other bilateral and multilateral engagements to promote and expand these policy pronouncements regarding responsible state behavior in cyberspace.

Organization for Security and Cooperation in Europe (OSCE)

As a result of the leadership by the United States and like-minded countries, the 57 member states of the OSCE, which includes not only Western allies but also Russia and other former Soviet states, reached consensus in March 2016 on an expanded set of CBMs. This expanded set, which includes five new CBMs, builds upon the 11 CBMs announced by the OSCE in 2013 that member states are already working to implement.

The initial 11 CBMs were primarily focused on building transparency and putting in place mechanisms for de-escalating conflict. For example, there were CBMs calling upon participating states to identify points of contact that foreign governments could reach out to in the event of a cyber incident emanating from the state's territory and put in place consultation and mediation mechanisms. The additional five CBMs focused more on cooperative measures focusing on issues like cybersecurity of critical infrastructure and developing public-private partnerships. Secure and resilient critical infrastructure, including in the communications sector, requires the integration of cyber, physical, and human elements. Since most critical infrastructure is privately owned, public-private partnerships are essential for strengthening critical infrastructure. Given the distributed nature of critical infrastructure, these efforts also require international collaboration. Work will continue this year to strengthen implementation of the previous CBMs and to begin implementing the new ones as well. This will build on the cooperation we have underway with many international partners in this and other similar fora. We also hope that this further success within the OSCE context can serve to strengthen CBMs as a model that other regional security organizations can adopt.

In addition to our work with governmental organizations, the Department of State engages extensively with a range of stakeholders outside of government, who play critical roles in helping to preserve and promote the same vision of cyberspace held by the United States. Non-government stakeholders are often part of our delegations to key meetings, for which there is intensive consultation, and we often engage with our stakeholders before and after key events to hear their views and to inform them of our activities. We also engage extensively with the stakeholder community ahead of and immediately following major cyber conferences, such as the Global Conference on Cyberspace, most recently in The Hague, the Netherlands, and previously in Seoul, South Korea.

Policy Challenge: Alternative Views of the Internet

A challenge to the implementation of our cyberspace strategy is a competing and alternative view of the Internet. The United States and much of the broader international community support the open flow and movement of data on the Internet that drives economic growth, protects human rights, and promotes innovation. The United States believes in a multistakeholder approach whereby governments, private sector, civil society, and the technical and academic communities cooperate to address both technical and policy threats through inclusive, transparent, consensus-driven processes.

China's approach to cyberspace in the international context is propelled by its desire to maintain internal stability, maintain sovereignty over its domestic cyberspace, and combat what it argues

is an emerging cyber arms race and 'militarization' of cyberspace. China has been willing to consider cyber confidence building measures, and has affirmed that international law applies in cyberspace, but has not been willing to affirm more specifically the applicability of the law of armed conflict or other laws of war, because it believes it would only serve to legitimize state use of cyber tools as weapons of war.

This has led to a set of external policies that reinforces traditional Chinese foreign policy priorities of non-interference in internal affairs, national sovereignty over cyberspace, and "no first use" of weapons. China views its expansive online censorship regime – including technologies such as the Great Firewall – as a necessary defense against destabilizing domestic and foreign influences, and it has promoted this conception internationally. China also urges creation of new "cyber governance" instruments, which would, inter alia, create new binding rules designed to limit the development, deployment, and use of "information weapons," promote speech and content controls, seek to replace the framework of the Council of Europe Convention on Cybercrime (Budapest Convention), elevate the role of governments vis-à-vis other stakeholders, and likely give the United Nations authority for determining attribution and responding to malicious cyber activity. While the United States and its partners seek to focus our cyber policy efforts on combatting threats to networks, cyber infrastructure, and other physical threats from cyber tools, China also emphasizes the threats posed by online content. In addition, some of these policies stand in sharp contrast to the U.S. view that all stakeholders should be able to contribute to the making of public policy regarding the Internet.

Russia's approach to cyberspace in the international context has focused on the maintenance of internal stability, as well as sovereignty over its "information space." While Russia co-authored the Code of Conduct, with China and other Shanghai Cooperation Organization members, Russia's ultimate goal is also a new international cyber convention, which they pair with criticism of the Budapest Convention.

Russia has nonetheless found common ground with the United States on our approach of promoting the applicability of international law to state conduct in cyberspace as well as voluntary, non-binding norms of state behavior in peacetime. Russia has also committed to the first ever set of bilateral cyber confidence building measures with the United States, as well as the first ever set of cyber CBMs within a multilateral institution, at the OSCE in 2013 and 2016 that I previously discussed.

We counter these alternative concepts of cyberspace policy through a range of diplomatic tools that include not only engagement in multilateral venues, but also direct bilateral engagement and awareness-raising with a variety of state and non-state actors. I now would like to discuss some of the technical challenges and threats the United States faces and some of the tools we have to respond to and prevent cyber incidents.

Responding to and Preventing Cyber Incidents

Continuing Cyber Threats

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity. In 2015, high profile cyber incidents included the breach of health insurance company Anthem, Inc.'s IT system that resulted in the theft of account information for millions of customers; an unauthorized breach of the Office of Personnel Management's systems that resulted in the theft of approximately 22 million personnel files; and hackers launching an unprecedented attack on the Ukraine power grid that cut power to hundreds of thousands of customers.

Overall, the unclassified information and communications technology networks that support U.S. government, military, commercial, and social activities remain vulnerable to espionage and

disruption. As the Department noted in the Strategy we submitted last month, however, the likelihood of a catastrophic attack against the United States from any particular actor is remote at this time. The Intelligence Community instead foresees an ongoing series of low-to-moderate level cyber operations from a variety of sources, which will impose cumulative costs on U.S. economic competitiveness and national security, pose risks to Federal and private sector infrastructure in the United States, infringe upon the rights of U.S. intellectual property holders, and violate the privacy of U.S. citizens.

In February, Director of National Intelligence James Clapper testified before Congress on the 2016 Worldwide Threat Assessment of the U.S. Intelligence Community, and stated: "Many actors remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences." He highlighted the malicious cyber activities of the leading state actors, non-state actors such as Da'esh, and criminals who are developing and using sophisticated cyber tools, including ransomware for extortion and malware to target government networks.

The Intelligence Community continues to witness an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the gains for the perpetrators.

Tools Available to Counter Cyber Threats

The United States works to counter technical challenges through a whole-of-government approach that brings to bear its full range of instruments of national power and corresponding policy tools – diplomatic, law enforcement, economic, military, and intelligence – as appropriate and consistent with applicable law.

The United States believes that deterrence in cyberspace is best accomplished through a combination of "deterrence by denial" – reducing the incentive of potential adversaries to use cyber capabilities against the United States by persuading them that the United States can deny their objectives – and "deterrence through cost imposition" – threatening or carrying out actions to inflict penalties and costs against adversaries that conduct malicious cyber activity against the United States. It is important to note that there is no one-size-fits-all approach to deterring or responding to cyber threats. Rather, the individual characteristics of a particular threat determine the tools that would most appropriately be used.

The President has at his disposal a number of tools to carry out deterrence by denial. These include a range of policies, regulations, and voluntary standards aimed at increasing the security and resiliency of U.S. government and private sector computer systems. They also include incident response capabilities and certain law enforcement authorities.

With respect to cost imposition, the President is able to draw on a range of response options from across the United States government.

Diplomatic tools provide a way to communicate to adversaries when their actions are unacceptable and to build support and greater cooperation among, or seek assistance from, allies and like-minded countries to address shared threats. Diplomatic démarches to both friendly and potentially hostile states have become a regular component of the United States' response to major international cyber incidents. In the longer term, U.S. efforts to promote principles of responsible state behavior in cyberspace, including peacetime norms, are intended to build increasing consensus among like-minded states that can form a basis for cooperative responses to irresponsible state actions.

Law enforcement tools can be used to investigate crimes and prosecute malicious cyber actors both within the United States and abroad. International cooperation is critical to cybercrime investigations, which is why the United States has promoted international harmonization of substantive and procedural cybercrime laws through the Budapest Convention, created an informal channel for data preservation and information sharing through the G7 24/7 network, and promoted donor partnerships to assist developing nations.

Economic tools, such as financial sanctions, may be used as a part of the broader U.S. strategy to change, constrain, and stigmatize the behavior of malicious actors in cyberspace. Since January 2015, the President has provided guidance to the Secretary of the Treasury to impose sanctions to counter North Korea's malicious cyber-enabled activities. Executive Order 13687 was issued, in part, in response to the provocative and destructive attack on Sony Pictures Entertainment, while Executive Order 13722 targets, among others, significant activities by North Korea to undermine cybersecurity, in line with the recently-signed North Korea Sanctions and Policy Enhancement Act of 2016. Aside from these North Korea-specific authorities, in April 2015, the President issued Executive Order 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, which authorizes the imposition of sanctions against persons whose malicious cyber-enabled activities could pose a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Military capabilities provide an important set of options for deterring and responding to malicious cyber activity. The Department of Defense continues to build its cyber capabilities and strengthen its cyber defense and deterrence posture. As part of this effort, the Department of Defense is building its Cyber Mission Force, which is already employing its capabilities to defend Department of Defense networks, defend the Nation against cyberattacks of significant consequence, and generate integrated cyberspace effects in support of operational plans and contingency operations. In addition, Secretary of Defense Ashton Carter announced earlier this year that U.S. forces are using cyber tools to disrupt Da'esh's command and control systems and to negatively impact its networks.

Intelligence capabilities are also an important tool at the President's disposal in detecting, responding to, and deterring malicious activities in cyberspace, particularly given the unique challenges associated with attributing and understanding the motivation behind such malicious activities.

Even with this broad range of tools, deterring cyber threats remains a challenge. Given the unique characteristics of cyberspace, the United States continues to work to develop additional and appropriate consequences that it can impose on malicious cyber actors.

Capacity Building

In addition to the tools that I have just outlined, the ability of the United States to respond to foreign cyber threats and fight transnational cybercrime is greatly enhanced by the capabilities and strength of our international partners in this area. Therefore, the Department of State is working with departments and agencies, allies and multilateral partners to build the capacity of foreign governments, particularly in developing countries, to secure their own networks as well as investigate and prosecute cybercriminals within their borders. The Department also actively promotes donor cooperation, including bilateral and multilateral participation in joint cyber capacity building initiatives.

In 2015, for example, the United States joined the Netherlands in founding the Global Forum on Cyber Expertise, a global platform for countries, international organizations, and the private sector to exchange best practices and expertise on cyber capacity building. The United States

partnered with Japan, Australia, Canada, the African Union Commission, and Symantec on four cybersecurity and cybercrime capacity building initiatives. The Department also provided assistance to the Council of Europe, the Organization of American States, and the United Nations Global Program on Cybercrime to enable delivery of capacity building assistance to developing nations. Many traditional bilateral law enforcement training programs increasingly include cyber elements, such as training investigators and prosecutors in the handling of electronic evidence. Much of our foreign law enforcement training on combating intellectual property crime focuses on digital theft.

In another example of capacity building, the Department of State, through its Bureau of International Narcotics and Law Enforcement Affairs, manages five International Law Enforcement Academies (ILEAs) worldwide, and one additional Regional Training Center. These six facilities provide law enforcement training and instruction to law enforcement officials from approximately 85 countries each year. The ILEA program includes a wide variety of cyber investigation training courses, from basic to advanced levels, taught by subject matter experts from the U.S. Secret Service and other agencies and policy-level discussions with senior criminal justice officials. This serves as a force multiplier to enhance the capabilities of the international law enforcement community to collaborate in the effort to fight cybercrime.

The Department of State is committed to continuing its capacity building initiatives as another effective way to counter international cyber threats and promote international cyber stability.

Looking ahead

Cybersecurity will continue to be a challenge for the United States when we take into consideration the rapidly expanding environment of global cyber threats, the increasing reliance on information technology and number of "smart devices," the reality that many developing nations are still in the early stages of their cyber maturity, and the ongoing and increasingly sophisticated use of information technology by terrorists and other criminals. Thus, the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic and capacity building efforts for the foreseeable future.

The Department will continue to spearhead the effort to promote international consensus that existing international law applies to state actions in cyberspace and build support for certain peacetime norms through assisting states in developing technical capabilities and relevant laws and policies, to ensure they are able to properly meet their commitments on norms of international cyber behavior.

Source: https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm, accessed 25 July 2018.

C. Presidential Executive Order on Strengthening Cybersecurity

On 11 May 2017, President Trump signed an executive order aimed at strengthening cybersecurity. The following is an excerpt from a White House News Release providing an overview of the order, the Executive Order can be found at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal:

FACT SHEET – President Trump Protects America's Cyber Infrastructure – 12 May 2017

"To truly make America safe, we truly have to make cybersecurity a major priority."

– Donald J. Trump

AMERICA'S NETWORK LEFT VULNERABLE: The United States has been left vulnerable to destructive attacks through cyber space. The President is following through on his campaign promise to keep America safe, even in cyberspace.

- The Federal Government, as a large and lucrative target for electronic criminals and foreign agents, has been a victim of cyber intrusions for years.
- The cybersecurity of critical American network infrastructure – public and private alike – is under constant attack from both foreign and domestic sources.
- On a daily basis we receive new reports of major corporations in the United States have been hacked by foreign-based threats.

TAKING ACTION TO SECURE OUR NATION'S CYBER DEFENSES: President Donald J. Trump signed an Executive Order to take much needed action to address cybersecurity vulnerabilities.

- In order to secure our Nation's defense, we are emphasizing Federal cybersecurity.
    - It is now the policy of the United States to manage cybersecurity risk as a Federal enterprise.
    - The President has mandated the use of the National Institute of Standards and Technology Cybersecurity Framework across government, ensuring the same high standards recommended for private industry are applied everywhere.
    - The Executive Order directs agency heads to begin planning for the deliberate modernization of Federal Executive Branch information technology (IT) – a critical, long overdue effort to better manage cyber risk. This work modernizing our IT will be championed from the White House by the President's American Technology Council.
    - Cabinet Secretaries and Agency Directors will be held accountable for managing cyber risk in their respective portfolios, ensuring accountability across the board.
    - The Government's information systems will be optimized, prioritizing modernity, safety, usability, and economy, innovating while addressing security. In this effort, the President has directed a preference towards shared services.
    - Specific actions include:
        - Requiring all agencies to use the industry-standard NIST Cybersecurity Framework (Framework) to manage their cybersecurity risks;
        - Requiring all agencies to prefer shared IT services in all future procurements, to the maximum extent allowed under the law;

        - Requiring all agencies to explicitly document their cybersecurity risk mitigation and acceptance choices, including any decisions to not mitigate known vulnerabilities in a timely manner, and describe their action plan in a report to implement the Framework, in a report to the Department of Homeland Security (DHS) and Office of Management and Budget (OMB);
        - Requiring the Secretary of DHS and the Director of OMB to evaluate the totality of these reports to comprehensively assess the adequacy of the Federal Government's overall cybersecurity risk management posture and propose changes in law, policy, and budgeting to protect adequately the executive branch enterprise;
        - Requiring the Secretary of Defense and the Director of National Intelligence to undertake comparable efforts for national security systems; and
        - Empowering the White House's American Technology Council to launch a process of planning for the deliberate modernization of Federal IT, including the technical feasibility and cost effectiveness of transitioning agencies to one or more consolidated network architectures and shared services such as email.
- Government and industry will partner in protecting our Nation's critical infrastructure.
    - As the private sector is heavily involved in our Nation's infrastructure, this Executive Order will prioritize deeper, more collaborative public-private partnerships in threat assessment, detection, protection, and mitigation.
        - Following the principle that "practice makes perfect," the President will work together with infrastructure providers to boost our national resilience to cyber-attacks through training exercises and other operations.
        - Voluntary compliance and collaborative efforts, such as efforts to address denial of service attacks, will be encouraged.
    - Specific actions include:
        - Establishing a clear policy that the Federal Government should bring to bear all of its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure.
        - Requiring civilian, military, and intelligence agencies to develop an integrated, comprehensive inventory of the specific legal authorities and capabilities that agencies could employ to support the cybersecurity risk management efforts of those critical infrastructure entities at greatest risk of attacks that could result in catastrophic impacts;
        - Requiring these agencies to offer such support to these entities on a voluntary basis, and to work directly with these entities to solicit their feedback and input on any gaps in the Federal Government's cybersecurity toolkit, including gaps in law, policy, or budgeting;
        - Evaluating Federal Government efforts to promote transparency in cybersecurity risk management practices within critical infrastructure to support market-driven risk management decisions;

        - Convening the private sector to address complex Internet of Things (IoT) cybersecurity challenges, starting with denial of service attacks perpetrated by IoT devices;
        - Strengthening the Nation's ability to respond to and recover from a prolonged power outage caused by a cyber-attack; and
        - Mitigating cybersecurity risks to Department of Defense weapons platforms and the defense industrial base, including risks associated with foreign manufacture of sensitive components.

- The Executive Order will strengthen our deterrence posture as a Nation and forge international coalitions to fight back against cyberattacks across the globe.
    - The White House, State Department, and all other applicable Federal agencies will continue to work hand-in-hand with the nations of the world to promote an open, interoperable, reliable, and secure global Internet. The Internet is a United States invention, it should reflect American values as it continues to transform the future for all nations and all generations.
        - The State Department shall be tasked with drafting an international engagement strategy for cybersecurity, outlining America's path forward with our allies.
    - The global shortage of cybersecurity professionals must be addressed, the President is committed to working programs that identify, develop, and retain first-class cyber security talent.
    - Other nations will not be allowed to hold us at risk through the use of cyber-attacks, espionage, or other malicious action.
    - Specific actions include:
        - Formulating strategic options for deterring adversaries and better protecting the American people from cyber threats;
        - Crafting an international engagement strategy for cybersecurity that will outline how the United States will take the initiative and work with partners to defend against and deter malicious actors, promote an international framework for cyber stability, and safeguard an open, interoperable and secure Internet that drives economic and social growth and development in the United States and around the world; and
        - Undertaking a comprehensive review of United States efforts in both the public and private sectors to support the development and sustainment of world-class civilian and military cybersecurity workforces, and benchmarking these efforts against parallel efforts by foreign governments to support their workforces.

Source – White House Fact Sheet: https://www.whitehouse.gov/briefings-statements/president-trump-protects-americas-cyber-infrastructure/, accessed 25 July 2018.

D. Departmental Responses to Executive Order on Strengthening Cybersecurity

This section includes U.S. Government departments' responses to President Trump's Cybersecurity Executive Order. Access to these responses can be found on the Department of State website: https://www.state.gov/s/cyberissues/eo13800/ and the Department of Homeland Security website: https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

1. **Recommendations to the President on Protecting American Cyber Interests Through International Engagement** (Excerpt).

The U.S. Vision for Cyberspace and Approach to Cyberspace Policy

U.S. national security interests, continued U.S. economic prosperity and leadership, and the continued preeminence of liberal democratic values hinge on the security, interoperability, and resilience of cyberspace. U.S. innovation, economic growth, and competitiveness depend on global trust in the Internet and confidence in the security and stability of the networks, platforms and services that compose cyberspace. The global nature of cyberspace necessitates robust international engagement and collaboration to accomplish U.S. government goals. Accordingly, the U.S. government pursues international cooperation in cyberspace to promote its vision of an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Through international engagement, the U.S. government seeks to ensure that the Internet and other connected networks and technologies remain valuable and viable tools for future generations.

U.S. Objectives for Cyberspace Policy

Through cooperation with foreign partners and allies, and engagement with all stakeholders as appropriate, the United States will pursue the following five objectives and corresponding actions to achieve its vision for cyberspace:

1. Increase international stability and reduce the risk of conflict stemming from the use of cyberspace by:

a. Promoting international commitments regarding what constitutes acceptable and unacceptable state behavior in cyberspace from all states and how international law applies to cyberspace;

b. Developing and implementing cyber confidence building measures (CBMs) in bilateral and regional security venues; and,

c. Promoting a new cooperative framework in support of cyber deterrence and cost imposition on malicious state actors and state-sponsored malicious activity.

2. Identify, detect, disrupt, and deter malicious cyber actors; protect, respond to, and recover from threats posed by those actors; and enhance the resilience of the global cyber ecosystem, including critical infrastructure, by:

a. Enhancing information sharing, including through automation and Computer Security Incident Response Team (CSIRT) channels;

b. Managing cyber crises and responding effectively to significant cyber incidents;

c. Improving cooperation to manage systemic cyber risk in an evolving global environment and strengthening public-private international cooperation to protect and build resilience in critical infrastructure;

d. Promoting cybersecurity education, training, and workforce development globally to address current and future cybersecurity challenges;

e. Prioritizing robust law enforcement cooperation;

f. Advancing military cyber cooperation; and,

g. Furthering cooperation on sensitive cyber intelligence issues with our partners and allies.

3. Uphold an open and interoperable Internet where human rights are protected and freely exercised and where cross-border data flows are preserved by:

a. Defending access to an open and interoperable Internet in multilateral and international fora where it is challenged;

b. Leveraging the existing coalition of like-minded countries that works to advance Internet freedom through diplomatic coordination; and,

c. Supporting global Internet freedom programs that fund civil society organizations on technology development, digital safety training, policy advocacy, and applied research.

4. Maintain the essential role of non-governmental stakeholders in how cyberspace is governed by:

a. Promoting the existing multistakeholder Internet governance system to manage key Internet resources and oppose new top-down or intergovernmental mechanisms for Internet governance; and,

b. Supporting the continued development, adoption, and use of interoperable, voluntary, consensus-based industry-driven technical standards.

5. Advance an international regulatory environment that supports innovation and respects the global nature of cyberspace by:

a. Preserving a flexible, risk-management approach to cybersecurity in the global marketplace;

b. Rejecting undue market access restrictions, including data localization requirements;

c. Advocating for a fair and competitive global market for U.S. businesses;

d. Encouraging private sector innovation to address security risks across the digital ecosystem; and,

e. Maintaining a strong and balanced intellectual property protection system that includes adequate and effective enforcement of intellectual property rights, while promoting innovation.

Source – Full Report: https://www.state.gov/documents/organization/282224.pdf, accessed 25 July 2018.

2. **Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats (**Excerpt).

Strategic Options

Deterrence by denial through defense and protection of critical infrastructure and other sensitive computer networks and ensuring efficient mitigation and timely recovery from malicious cyber activities must be foundational to the U.S. deterrence approach. The United States will continue to enhance its efforts to deny adversaries the benefits of their malicious cyber activities.

At the same time, the United States recognizes that network defense alone will not be sufficient to deter determined and sophisticated state-sponsored adversaries. The United States will also undertake a new effort to increase deterrence of state actors through cost imposition and other measures.

The desired end states of U.S. deterrence efforts will be:

- A continued absence of cyber attacks that constitute a use of force against the United States, its partners, and allies; and
- A significant, long-lasting reduction in destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against U.S. interests that fall below the threshold of the use of force.

The President already has a wide variety of cyber and non-cyber options for deterring and responding to cyber activities that constitute a use of force. Credibly demonstrating that the United States is capable of imposing significant costs on those who carry out such activities is indispensable to maintaining and strengthening deterrence.

With respect to activities below the threshold of the use of force, the United States should, working with likeminded partners when possible, adopt an approach of imposing swift, costly, and transparent consequences on foreign governments responsible for significant malicious cyber activities aimed at harming U.S. national interests. Key elements of the approach will include:

1. **Creating a policy for when the United States will impose consequences**: The policy should provide criteria for the types of malicious cyber activities that the U.S. government will seek to deter. The outlines of this policy must be communicated publicly and privately in order for it to have a deterrent effect.

2. **Developing a range of consequences**: The United States should prepare a menu of options for swift, costly, and transparent consequences below the threshold of the use of force that it can impose, consistent with U.S. obligations and commitments, following an incident that merits a strong response that can have downstream deterrent effects. As the United States develops these options, it should assess and seek to minimize the potential risks and costs associated with each of them.

3. **Conducting policy planning for imposing these consequences**: In addition to developing consequences themselves, the United States should conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences. Such planning, which should include the development of appropriate interagency response procedures, will help ensure consistent responses to different incidents and assist in managing the risk of escalation.

4. **Building partnerships**: The imposition of consequences would be more impactful and send a stronger deterrent message if it were carried out in concert with partners.

Partner states could, on a voluntary basis, support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident, and/or actual participation in the imposition of consequences against perpetrator governments.

Source – Full Report: https://www.state.gov/documents/organization/282253.pdf, accessed 25 July 2018.

3. **Support to Critical Infrastructure at Greatest Risk.**

DHS, in coordination with relevant Sector-Specific Agencies (SSAs), annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Section 9 of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, utilizing a risk-based approach. These "Section 9 entities" own or operate critical infrastructure "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

DHS, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the heads of appropriate Sector-Specific Agencies, identified authorities and capabilities that the Federal Government could employ to support the cybersecurity efforts of Section 9 entities. Additionally, DHS and its partners engaged these entities to evaluate how the authorities and capabilities might be employed to support cybersecurity risk management efforts.

The findings and recommendations from this work were reported to the President for better supporting the Section 9 entities in their cybersecurity risk management efforts, to include:

- Establishing a DHS program office to strengthen support to Section 9 entities and improve coordination of interagency support;
- Enhancing access to classified information;
- Revisiting the methodology to explore a more functions-based approach to identifying Section 9 entities;
- Improving incident communication and coordination;
- Improving cross-sector information sharing with Section 9 entities;
- Exploring incentives for private sector entities to exercise due care in protecting their information and information systems which could include reporting cybersecurity incidents to the Government;
- Establishing a public-private initiative to counter supply chain vulnerabilities and reduce cybersecurity vendor risk; and
- Exploring new technology to reduce cyber risk.

DHS will lead an interagency working group to focus on implementing the recommendations and engage with each Section 9 entity to ensure its understanding of the programs and resources available.

Source – Full Report: https://www.dhs.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary, accessed 25 July 2018.

4. **Supporting Transparency in the Marketplace.**

DHS, in coordination with the Department of Commerce, was directed to examine the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices, with a focus on publicly traded critical infrastructure entities. The resulting report was developed in a short 90-day timeframe through a collaborative interagency process; limited private industry engagement; and a literature review of secondary sources addressing the sufficiency of existing Federal policies and practices in promoting transparency of cybersecurity risks and risk management practices and the effectiveness of transparency systems generally in advancing policy goals. There were 96 different sources identified as part of the literature review, and several Federal policies and practices identified. The associated findings provide insight into the effectiveness of transparency systems; the sufficiency of existing Federal policies and practices; and informs future policy discussions regarding market transparency and improving cybersecurity outcomes.

Source – Full Report: https://www.dhs.gov/publication/supporting-transparency-marketplace-summary, accessed 25 July 2018.

5. **Resilience Against Botnets and Other Automated, Distributed Threats**.

DHS worked closely with the Department of Commerce to lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and Communications Ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetuated by automated and distributed attacks.

The report, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, summarizes the opportunities and challenges in reducing the botnet threat, and offers supporting actions to be taken by both the Government and private sector in order to reduce the threat of automated, distributed attacks. The report is centered around six principal themes:

- Automated, distributed attacks are a global problem.
- Effective tools exist, but are not widely used.
- Products should be secured during all stages of the lifecycle.
- Awareness and education is needed.
- Market incentives should be more effectively aligned.
- Automated, distributed attacks are an ecosystem-wide challenge.

Created with broad input from stakeholders and experts, the report lists five complementary goals that would improve the resilience of the Internet ecosystem. The recommended actions include ongoing activities that should be continued or expanded, as well as new initiatives, such as an effort to increase software component transparency and a public campaign to support awareness of IoT security.

Source – Full Report: https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets, accessed 25 July 2018.

6. **Assessment of Electricity Disruption Incident Response Capabilities**

DHS also worked closely with the Department of Energy to conduct an assessment of the potential scope and duration of a prolonged power outage associated with a

significant cyber incident, as well as an evaluation of the readiness and gaps in the United States' ability to manage and mitigate consequence s of a cyber incident against the electric subsector. This assessment concluded that the United States is, in general, well prepared to manage most electricity disruptions, though there are particular areas where catastrophic considerations and emerging threats reveal capability gaps against cyberattacks.

To address these gaps, the assessment outlines areas spanning from improving public communications across officials at all levels, expanding cybersecurity technical expertise and information sharing, and integrating and augmenting planning and analytic capabilities for long term disruption and potential consequences and impacts resulting from such a disruption. In addition, early integration of cybersecurity into system design; funding for cybersecurity investments, particularly for smaller utilities; and strong workforce development would holistically support national preparedness of the Nation's electric infrastructure.

Source – Full Report: https://www.dhs.gov/publication/section-2e-assessment-electricity-disruption-incident-response-capabilities, accessed 25 July 2018.

7. **American Cybersecurity Workforce Development**.

The Department of Commerce and DHS assessed the scope and sufficiency of past efforts to educate and train the future U.S. cybersecurity workforce and to provide a report that identifies findings and recommendations on how to support the growth and sustainment of these future cybersecurity employees in the public and private sectors. To accomplish this work, cybersecurity education and workforce development subject matter experts from the departments of Defense, Labor, and Education, as well as the Office of Personnel Management, the National Science Foundation, and other relevant agencies were convened to discuss and present the status of existing efforts to grow and expand the Nation's cybersecurity workforce pipeline. To ensure broad input, a public, national-level workshop was convened and a public request for information (RFI) was issued.

The interagency working group, led by the Department of Commerce's National Institute for Standards and Technology (NIST) and DHS, compiled the results into a report to the President, identifying four key findings: (1) the U.S. cybersecurity workforce needs immediate and sustained improvements; (2) it is necessary to expand the pool of cybersecurity candidates through retraining and by increasing the participation of women, minorities, and veterans; (3) there is a shortage of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors; and (4) comprehensive and reliable data about cybersecurity workforce position needs and education and training programs are lacking.

The report details five key recommendations to address the findings:

- The Federal Government should lead in launching a high-profile, national Call to Action to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs;
- The Administration should focus on, and recommend, long-term authorization and sufficient appropriations for high-quality, effective cybersecurity education and workforce development programs;
- The private and public sectors should transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce

through retraining, hands-on, experiential and work-based learning approaches, including apprenticeships, research experiences, co-op programs, internships, virtual training and assessment environments, and by providing greater financial assistance for cybersecurity education and training;

- The private and public sectors should align education and training with employers' cybersecurity workforce needs by applying the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, developing cybersecurity career model paths, and establishing a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives; and
- The private and public sectors should establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments through robust metrics and evaluation mechanisms to track and determine the quantity and quality of individuals educated, trained, and ready to fulfill cybersecurity tasks in the workplace.

Source – Full Report: https://www.dhs.gov/publication/supporting-growth-and-sustainment-nations-cybersecurity-workforce, accessed 25 July 2018.

II. Department of Homeland Security Strategy and Guidance

A. The Cybersecurity Strategy for the Homeland Security Enterprise

Department of Homeland Security (DHS) released this strategy on 15 May 2018. The Cybersecurity Strategy Fact Sheet is provided below, the full document can be found at: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

U.S. Department of Homeland Security
Cybersecurity Strategy

INTRODUCTION

We depend upon cyberspace for daily conveniences, critical services, and economic prosperity. At the U.S. Department of Homeland Security, we believe that cyberspace can be made secure and resilient. DHS works with key partners across the Federal government, State and local governments, industry, and the international community to identify and manage national cybersecurity risks. The DHS Cybersecurity Strategy sets out five pillars of a DHS-wide risk management approach and provides a framework for executing our cybersecurity responsibilities and leveraging the full range of the Department's capabilities to improve the security and resilience of cyberspace.

Reducing our national cybersecurity risk requires an innovative approach that fully leverages our collective capabilities across the Department and the entire cybersecurity community. DHS will strive to better understand our national cybersecurity risk posture, and engage with key partners to collectively address cyber vulnerabilities, threats, and consequences. We will build on ongoing efforts to reduce and manage vulnerabilities of federal networks and critical infrastructure to harden them against attackers. We will reduce threats from cyber criminal activity through prioritized law enforcement intervention. We will seek to mitigate the consequences from cybersecurity incidents that do occur. Finally, we will engage with the global cybersecurity community to strengthen the security and resiliency of the overall cyber ecosystems by addressing systemic challenges like increasingly global supply chains; by fostering improvements in international collaboration to deter malicious cyber actors and build capacity; by increasing research and development, and by improving our cyber workforce.

Through these efforts we seek to create a safe and secure cyberspace for the American people and protect the open, interoperable, secure and resilient Internet.

DHS CYBERSECURITY GOALS

Pillar I Risk Identification

Goal 1: Assess Evolving Cybersecurity Risks.

We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.

Pillar II Vulnerability Reduction

Goal 2: Protect Federal Government Information Systems.

We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.

Goal 3: Protect Critical Infrastructure.

We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.

Pillar III Threat Reduction

Goal 4: Prevent and Disrupt Criminal Use of Cyberspace.

We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.

Pillar IV Consequence Mitigation

Goal 5: Respond Effectively to Cyber Incidents.

We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.

Pillar V Enable Cybersecurity Outcomes

Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem.

We will support policies and activities that enable improved global cybersecurity risk management.

Goal 7: Improve Management of DHS Cybersecurity Activities.

We will execute our departmental cybersecurity efforts in an integrated and prioritized way.

OUR CYBERSECURITY STRATEGY IN ACTION

- In October 2017, DHS issued Binding Operational Directive 18-01, mandating that Federal agencies take specific steps to enhance email and web security, including the deployment of DMARC (Domain-based Message Authentication, Reporting and Conformance).
- During the 2017 WannaCry worldwide malware attack, the National Protection and Programs Directorate (NPPD) partnered with other agencies and industry to assist U.S. hospitals to ensure their systems were not vulnerable, and issued a public technical alert to assist defenders with defeating this malware.
- In January 2018, the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and the Department of Justice in Las Vegas indicted 36 individuals for their roles in the Infraud Organization, an internet-based criminal enterprise engaged in the large scale acquisition and sale of stolen credit card data and identity documents. This organization was responsible for the loss in excess of $530 million. The HSI investigation has led to the recovery of over 4.3 million compromised credit card account numbers.
- In July 2017, the United States Secret Service, through a synchronized international law enforcement operation, affected the arrest of a Russian national alleged to have operated BTC-e. From 2011 to 2017, BTC-e is alleged with facilitating over $4 billion worth of bitcoin transactions worldwide for cyber criminals engaging in computer hacking, identity theft, ransomware, public corruption, and narcotics distribution. Researchers estimate approximately 95% of ransomware payments were laundered through BTC-e.
- In October 2017, the U.S. Coast Guard (USCG) stood up the Office of Cyberspace Forces, to organize, man, train, and equip the USCG cyberspace operational workforce and develop cyberspace operational policy to operate, maintain, defend, and secure USCG systems and networks, enable USCG operations through cyberspace capabilities, and protect the Maritime Transportation System from cyber threats.

Source DHS Fact Sheet: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf, accessed 25 July 2018.

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: https://www.nist.gov/sites/default/files/documents/cyberframework/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: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed 25 July 2018.

III. Department of Justice Cyber Strategy and Guidance

A. DOJ 2018 Report of the Attorney General's Cyber-Digital Task Force

The following is an excerpt from Report of the Attorney Generals Cyber-Digital Task Force (July 2018). The report can be found at: https://www.justice.gov/ag/page/file/1076696/download.

Introduction

In February 2018, the Attorney General established a Cyber-Digital Task Force within the Department and directed the Task Force to answer two basic, foundational questions: How is the Department responding to cyber threats? And how can federal law enforcement more effectively accomplish its mission in this important and rapidly evolving area?

This report addresses the first question. It be- gins by focusing on one of the most pressing cyber-enabled threats our Nation faces: the threat posed by malign foreign influence operations. Chapter 1 explains what foreign influence operations are, and how hostile foreign actors have used these operations to tar- get our Nation's democratic processes, including our elections. This chapter concludes by describing the Department's protective efforts with respect to the upcoming 2018 midterm elections, and announces a new Department policy grounded in our longstanding principles of political neutrality, adherence to the rule of law, and safeguarding the public trust that governs the disclosure of foreign influence operations.

Chapters 2 and 3 discuss other cyber-enabled threats our Nation faces, particularly those connected with cybercrimes. These chapters describe the resources the Department is deploying to confront those threats, and how our efforts further the rule of law in this country and around the world. Chapter 4 focuses on a critical aspect of the Department's mission, in which the Federal Bureau of Investigation plays a lead role: responding to cyber incidents. Chapter 5 then turns the lens inward, focusing on the Department's efforts to recruit and train our own personnel on cyber matters. Finally, the report concludes in Chapter 6 with thoughts and observations about certain priority policy matters, and charts a path for the Task Force's future work. Over the next few months, the Department will build upon this initial report's findings, and will provide recommendations to the Attorney General for how the Department can even more efficiently manage the growing global cyber challenge.

Source: https://justice.gov/cyberreport, accessed 25 July 2018.

IV. Department of Defense Strategy and Guidance

A. DOD Cyber Strategy

DOD released its Cyber Strategy in September 2018. The following is the introduction to the Department of Defense Cyber Strategy Summary. The full document can be found at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

INTRODUCTION

American prosperity, liberty, and security depend upon open and reliable access to information. The Internet empowers us and enriches our lives by providing ever-greater access to new knowledge, businesses, and services. Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control.

The arrival of the digital age has also created challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the Internet that we seek to protect creates significant vulnerabilities. Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.

We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.

The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests.

During wartime, U.S. cyber forces will be prepared to operate alongside our air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Force. Adversary militaries are increasingly reliant on the same type of computer and network technologies that have become central to Joint Force warfighting. The Department will exploit this reliance to gain military advantage. The Joint Force will employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict.

The *2018 Department of Defense Cyber Strategy* represents the Department's vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. It supersedes the *2015 DoD Cyber Strategy*.

The United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day. We must assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict. Our Soldiers, Sailors, Airmen, Marines, and civilian employees stand ready, and we will succeed.

STRATEGIC COMPETITION IN CYBERSPACE

The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

First, we must ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace. This is a foundational requirement for U.S. national security and a key to ensuring that we deter aggression, including cyber attacks that constitute a use of force, against the United States, our allies, and our partners. The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI)[1] and Defense Industrial Base (DIB)[2] entities. We will defend forward to halt or degrade cyberspace operations targeting the Department, and we will collaborate to strengthen the cybersecurity and resilience of DoD, DCI, and DIB networks and systems.

Second, the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies.

Third, the Department will work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests.

The Department's cyberspace objectives are:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;[3]
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

DEFENDING CIVILIAN ASSETS THAT ENABLE U.S. MILITARY ADVANTAGE

The Department must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. Our chief goal in maintaining an ability to defend DCI is to ensure the infrastructure's continued functionality and ability to support DoD objectives in a contested cyber environment. Our focus working with DIB entities is to protect sensitive DoD information whose loss, either individually or in aggregate, could result in an erosion of Joint Force military advantage. As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

Endnotes

[1] **"Defense Critical Infrastructure"** refers to the composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide (Department of Defense Directive 3020.40).

[2] **"Defense Industrial Base"** refers to the Department, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements (32 CFR Part 236).

[3] **"Significant cyber incident"** refers to an event occurring on or conducted through a computer network that is (or a group of related events that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people (Presidential Policy Directive 41).

Source: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed 1 November 2018.

V. U.S. Cyber Law Guidance

A. DOS Position on International Law in Cyberspace

Remarks on International Law and Stability in Cyberspace

The following excerpt is from a presentation by Brian J. Egan, Legal Advisor, U.S. Department of State, made at Berkeley Law School, CA on 10 November 2016: https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

This is a fitting place to discuss the topic I am here to speak about today – the importance of international law and stability in cyberspace – just across the Bay from Silicon Valley, home to many of the world's largest and most innovative information technology companies. The remarkable reach of the Internet and the ever-growing number of connections between computers and other networked devices are delivering significant economic, social, and political benefits to individuals and societies around the world. In addition, an increasing number of States and non-State actors are developing the operational capability and capacity to pursue their objectives through cyberspace. Unfortunately, a number of those actors are employing their capabilities to conduct malicious cyber activities that cause effects in other States' territories. Significant cyber incidents – including many that are reportedly State-sponsored – frequently make headline news.

In light of this, it is reasonable to ask: could we someday reach a tipping point where the risks of connectivity outweigh the benefits we reap from cyberspace? And how can we prevent cyberspace from becoming a source of instability that could lead to inter-State conflict?

I don't think we will reach such a tipping point, but how we maintain cyber stability in order to preserve the continued benefits of connectivity remains a critical question. And international law, I would submit, is an essential element of the answer.

Existing principles of international law form a cornerstone of the United States' strategic framework of international cyber stability during peacetime and during armed conflict. The U.S. strategic framework is designed to achieve and maintain a stable cyberspace environment where all States and individuals are able to realize its benefits fully, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for States to engage in disruptive behavior or to attack one another.

There are three pillars to the U.S. strategic framework, each of which can help to ensure stability in cyberspace by reducing the risks of misperception and escalation. The first is global affirmation of the applicability of existing international law to State activity in cyberspace in both peacetime and during armed conflict. The second is the development of international consensus on certain additional voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which is of course the predominant context in which States interact. And the third is the development and implementation of practical confidence-building measures to facilitate inter-State cooperation on cyber-related matters. I'll address two of these pillars—international law and voluntary, non-binding norms—in greater detail today.

International Law

In September 2012, my predecessor, Harold Koh, delivered remarks on "International Law in Cyberspace" at U.S. Cyber Command's Legal Conference. It says a lot about where we were four years ago that the first two questions Koh addressed in his speech were as fundamental as: "Do established principles of international law apply to cyberspace?" and "Is cyberspace a law-free zone, where anything goes?" (So as not to leave you hanging, the answers to those questions are an emphatic "yes" and "no" respectively!)

We have made significant progress since then. One prominent forum in which these issues are discussed is the United Nations (UN) Group of Governmental Experts (GGE) that deals with cyber issues in the context of international security. The GGE is a body established by the UN Secretary-General with a mandate from the UN General Assembly to study, among other things, how international law applies to States' cyber activities, with a view to promoting common understandings. In 2013, the 15-State GGE recognized the applicability of existing international law to States' cyber activities. Just last year, the subsequent UN GGE on the same topic, expanded to include 20 States, built on the 2013 report and took an additional step by recognizing the applicability in cyberspace of the inherent right of self-defense as recognized in Article 51 of the UN Charter. The 2015 GGE report also recognized the applicability of the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction to the conduct of hostilities in and through cyberspace. With other recent bilateral and multilateral statements, including that of the leaders of the Group of Twenty (G20) States in 2015, we have seen an emerging consensus that existing international law applies to States' cyber activities.

Recognizing the applicability of existing international law as a general matter, however, is the easy part, at least for most like-minded nations. Identifying how that law applies to specific cyber activities is more challenging, and States rarely articulate their views on this subject publicly. The United States already has made some efforts in this area, including by setting forth views on the application of international law to cyber activities in Koh's 2012 speech and also in the U.S. submission to the 2014–15 UN GGE, both of which are publicly available in the Digest of U.S. Practice in International Law. The U.S. Department of Defense also has presented its views on aspects of this topic in its publicly available Law of War Manual. But more work remains to be done.

Increased transparency is important for a number of reasons. Customary international law, of course, develops from a general and consistent practice of States followed by them out of a sense of legal obligation, or opinio juris. Faced with a relative vacuum of public State practice and opinio juris concerning cyber activities, others have sought to fill the void with their views on how international law applies in this area. The most prominent and comprehensive of these efforts is the Tallinn Manual project. Although this is an initiative of the NATO Cooperative Cyber Defence Centre of Excellence, it is neither State-led nor an official NATO project. Instead, the project is a non-governmental effort by international lawyers who first set out to identify the international legal rules applicable to cyber warfare, which led to the publication of "Tallinn Manual 1.0" in 2013. The group is now examining the international legal framework that applies to cyber activities below the threshold of the use of force and outside of the context of armed conflict, which will result in the publication of a "Tallinn Manual 2.0" by the end of this year.

I commend the Tallinn Manual project team on what has clearly been a tremendous and thoughtful effort. The United States has unequivocally been in accord with the underlying premise of this project, which is that existing international law applies to State behavior in cyberspace. In this respect, the Tallinn Manuals will make a valuable contribution to underscoring and demonstrating this point across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals.

States must also address these challenging issues. Interpretations or applications of international law proposed by non-governmental groups may not reflect the practice or legal views of many or most States. States' relative silence could lead to unpredictability in the cyber realm, where States may be left guessing about each other's views on the applicable legal framework. In the context of a specific cyber incident, this uncertainty could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict.

To mitigate these risks, States should publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent possible in international and domestic forums. Specific cyber incidents provide States with opportunities to do this, but it is equally important – and often easier – for States to articulate public views outside of the context of specific cyber operations or incidents. Stating such views publicly will help give rise to more settled expectations of State behavior and thereby contribute to greater predictability and stability in cyberspace. This is true for the question of what legal rules apply to cyber activity that may constitute a use of force, or that may take place in a situation of armed conflict. It is equally true regarding the question of what legal rules apply to cyber activities that fall below the threshold of the use of force and take place outside of the context of armed conflict.

Although many States, including the United States, generally believe that the existing international legal framework is sufficient to regulate State behavior in cyberspace, States likely have divergent views on specific issues. Further discussion, clarification, and cooperation on these issues remains necessary. The present task is for States to begin to make public their views on how existing international law applies.

In this spirit, and building on Harold Koh's remarks in 2012 and the United States' 2014 and 2016 submissions to the UN GGE, I would like to offer some additional U.S. views on how certain rules of international law apply to States' behavior in cyberspace, beginning first with cyber operations during armed conflict, and then turning to the identification of voluntary, non-binding norms applicable to State behavior during peacetime.

Cyber Operations in the Context of Armed Conflict

Turning to cyber operations in armed conflict, I would like to start with the U.S. military's cyber operations in the context of the ongoing armed conflict with the Islamic State of Iraq and the Levant (ISIL). As U.S. Defense Secretary Ashton Carter informed Congress in April 2016, U.S. Cyber Command has been asked "to take on the war against ISIL as essentially [its] first major combat operation […] The objectives there are to interrupt ISIL command-and-control, interrupt its ability to move money around, interrupt its ability to tyrannize and control population[s], [and] interrupt its ability to recruit externally."

The U.S. military must comply with the United States' obligations under the law of armed conflict and other applicable international law when conducting cyber operations against ISIL, just as it does when conducting other types of military operations during armed conflict. To the extent that such cyber operations constitute "attacks" under the law of armed conflict, the rules on conducting attacks must be applied to those cyber operations. For example, such operations must only be directed against military objectives, such as computers, other networked devices, or possibly specific data that, by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Such operations also must comport with the requirements of the principles of distinction and proportionality. Feasible precautions must be taken to reduce the risk of incidental harm to civilian infrastructure and users. In the cyber context, this requires parties to a conflict to assess the potential effects of cyber activities on both military and civilian infrastructure and users.

Not all cyber operations, however, rise to the level of an "attack" as a legal matter under the law of armed conflict. When determining whether a cyber activity constitutes an "attack" for purposes of the law of armed conflict, States should consider, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question.

Even if they do not rise to the level of an "attack" under the law of armed conflict, cyber operations during armed conflict must nonetheless be consistent with the principle of military necessity. For example, 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. Additionally, even if a cyber operation does not rise to the level of an "attack" or does not cause injury or damage that would need to be considered under the principle of proportionality in conducting attacks, that cyber operation still should comport with the general principles of the law of war.

Other international legal principles beyond the rules and principles of the law of armed conflict that I just discussed are also relevant to U.S. cyber operations undertaken during armed conflict. As then-Assistant to the President for Homeland Security and Counterterrorism John Brennan said in his September 2011 remarks at Harvard Law School, "[i]nternational legal principles, including respect for a State's sovereignty […], impose important constraints on our ability to act unilaterally […] in foreign territories." It is to this topic—the role played by State sovereignty in the legal analysis of cyber operations—that I'd like to turn now.

Sovereignty and Cyberspace

In his remarks in 2012, Harold Koh stated that "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict." I would like to build on that statement and offer a few thoughts about the relevance of sovereignty principles to States' cyber activities.

As an initial matter, remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects.

Most States, including the United States, engage in intelligence collection abroad. As President Obama said, the collection of intelligence overseas is "not unique to America." As the President has also affirmed, the United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decisionmakers have access to timely, accurate, and insightful information. Indeed, the President issued a directive in 2014 to clarify the principles that would be followed by the United States in undertaking the collection of signals intelligence abroad.

Such widespread and perhaps nearly universal practice by States of intelligence collection abroad indicates that there is no per se prohibition on such activities under customary international law. I would caution, however, that because "intelligence collection" is not a defined term, the absence of a per se prohibition on these activities does not settle the question of whether a specific intelligence collection activity might nonetheless violate a provision of international law.

Although certain activities—including cyber operations—may violate another State's domestic law, that is a separate question from whether such activities violate international law. The United States is deeply respectful of other States' sovereign authority to prescribe laws governing activities in their territory. Disrespecting another State's domestic laws can have serious legal and foreign policy consequences. As a legal matter, such an action could result in the criminal prosecution and punishment of a State's agents in the United States or abroad, for example, for offenses such as espionage or for violations of foreign analogs to provisions such as the U.S. Computer Fraud and Abuse Act. From a foreign policy perspective, one can look to the consequences that flow from disclosures related to such programs. But such domestic law and

foreign policy issues do not resolve the independent question of whether the activity violates international law.

In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.

Relatedly, consider the challenges we face in clarifying the international law prohibition on unlawful intervention. As articulated by the International Court of Justice (ICJ) in its judgment on the merits in the Nicaragua Case, this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system. This is generally viewed as a relatively narrow rule of customary international law, but States' cyber activities could run afoul of this prohibition. For example, a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention. For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace.

Some may ask why it matters where the international community draws these legal lines. Put starkly, why does it matter whether an activity violates international law? It matters, of course, because the community of nations has committed to abide by international law, including with respect to activities in cyberspace. International law enables States to work together to meet common goals, including the pursuit of stability in cyberspace. And international law sets binding standards of State behavior that not only induce compliance by States but also provide compliant States with a stronger basis for criticizing – and rallying others to respond to – States that violate those standards. As Harold Koh stated in 2012, "[i]f 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." Working to clarify how international law applies to States' activities in cyberspace serves those ends, as it does in so many other critical areas of State activity.

Before leaving the topic of sovereignty, I'd like to address one additional related issue involving a State's control over cyber infrastructure and activities within, rather than outside, its territory. In his 2012 speech, Koh observed that "[t]he physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and is subject to the jurisdiction of the territorial State." However, he went on to emphasize that "[t]he exercise of jurisdiction by the territorial State, however, is not unlimited; it must be consistent with applicable international law, including international human rights obligations."

I want to underscore this important point. Some States invoke the concept of State sovereignty as a justification for excessive regulation of online content, including censorship and access restrictions, often undertaken in the name of counterterrorism or "countering violent extremism." And sometimes, States also deploy the concept of State sovereignty in an attempt to shield themselves from outside criticism.

So let me repeat what Koh made clear: Any regulation by a State of matters within its territory, including use of and access to the Internet, must comply with that State's applicable obligations under international human rights law.

There is no doubt that terrorist groups have become dangerously adept at using the Internet and other communications technologies to propagate their hateful messages, recruit adherents, and urge followers to commit violent acts. This is why all governments must work together to target online criminal activities – such as illicit money transfers, terrorist attack planning and coordination, criminal solicitation, and the provision of material support to terrorist groups. U.S. efforts to prevent the Internet from being used for terrorist purposes also focus on criminal activities that facilitate terrorism, such as financing and recruitment, not on restricting expressive content, even if that content is repugnant or inimical to our core values.

Such efforts must not be conflated with broader calls to restrict public access to or censor the Internet, or even – as some have suggested – to effectively shut down entire portions of the Web. Such measures would not advance our security, and they would be inconsistent with our values. The Internet must remain open to the free flow of information and ideas. Restricting the flow of ideas also inhibits spreading the values of understanding and mutual respect that offer one of the most powerful antidotes to the hateful and violent narratives propagated by terrorist groups.

That is why the United States holds the view that use of the Internet, including social media, in furtherance of terrorism and other criminal activity must be addressed through lawful means that respect each State's international obligations and commitments regarding human rights, including the freedom of expression, and that serve the objectives of the free flow of information and a free and open Internet. To be sure, the incitement of imminent terrorist violence may be restricted. However, certain censorship and content control, including blocking websites simply because they contain content that criticizes a leader, a government policy, or an ideology, or because the content espouses particular religious beliefs, violates international human rights law and must not be engaged in by States.

State Responsibility and the "Problem of Attribution" in Cyberspace

I have been talking thus far about States' activities and operations in cyberspace. But as many of you know, it is often difficult to detect who or what is responsible for a given cyber incident. This leads me to the frequently raised and much debated "problem of attribution" in cyberspace.

States and commentators often express concerns about the challenge of attribution in a technical sense – that is, the challenge of obtaining facts, whether through technical indicators or all-source intelligence, that would inform a State's determinations about a particular cyber incident. Others have raised issues related to political decisions about attribution – that is, considerations that might be relevant to a State's decision to go public and identify another State as the actor responsible for a particular cyber incident and to condemn that act as unacceptable. These technical and policy discussions about attribution, however, should be distinguished from the legal questions about attribution. In my present remarks, I will focus on the issue of attribution in the legal sense.

From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States. For example, cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to exercise governmental authority are attributable to that State, if such organs, persons, or entities are acting in that capacity.

Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own.

Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information – whether obtained through technical means or all-source intelligence – that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.

The law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution. In this context, a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not – and cannot be – required. Instead, international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.

I also want to note that, despite the suggestion by some States to the contrary, there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice – it is not compelled by international law.

Countermeasures and Other "Defensive" Measures

I want to turn now to the question of what options a victim State might have to respond to malicious cyber activity that falls below the threshold of an armed attack. As an initial matter, a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States. Such acts – which are known as acts of retorsion – may include, for example, the imposition of sanctions or the declaration that a diplomat is persona non grata.

In certain circumstances, a State may take action that would otherwise violate international law in response to malicious cyber activity. One example is the use of force in self-defense in response to an actual or imminent armed attack. Another example is that, in exceptional circumstances, a State may be able to avail itself of the plea of necessity, which, subject to certain conditions, might preclude the wrongfulness of an act if the act is the only way for the State to safeguard an essential interest against a grave and imminent peril.

In the time that remains, however, I would like to talk about a type of State response that has received a lot of attention in discussions about cyberspace: countermeasures. The customary international law doctrine of countermeasures permits a State that is the victim of an internationally wrongful act of another State to take otherwise unlawful measures against the responsible State in order to cause that State to comply with its international obligations, for example, the obligation to cease its internationally wrongful act. Therefore, as a threshold matter, the availability of countermeasures to address malicious cyber activity requires a prior internationally wrongful act that is attributable to another State. As with all countermeasures, this puts the responding State in the position of potentially being held responsible for violating international law if it turns out that there wasn't actually an internationally wrongful act that triggered the right to take countermeasures, or if the responding State made an inaccurate attribution determination. That is one reason why countermeasures should not be engaged in lightly.

Additionally, under the law of countermeasures, measures undertaken in response to an internationally wrongful act performed in or through cyberspace that is attributable to a State must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality, including the requirements that a countermeasure must be

designed to cause the State to comply with its international obligations – for example, the obligation to cease its internationally wrongful act – and must cease as soon as the offending State begins complying with the obligations in question.

The doctrine of countermeasures also generally requires the injured State to call upon the responsible State to comply with its international obligations before a countermeasure may be taken – in other words, the doctrine generally requires what I will call a "prior demand." The sufficiency of a prior demand should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement, which is to give the responsible State notice of the injured State's claim and an opportunity to respond.

I also should note that countermeasures taken in response to internationally wrongful cyber activities attributable to a State generally may take the form of cyber-based countermeasures or non-cyber-based countermeasures. That is a decision typically within the discretion of the responding State and will depend on the circumstances.

Voluntary, Non-Binding Norms of Responsible State Behavior in Peacetime

In the remainder of my remarks, I'd like to discuss very briefly another element of the United States' strategic framework for international cyber stability: the development of international consensus on certain additional voluntary, non-binding norms of responsible State behavior in cyberspace that apply during peacetime.

Internationally, the United States has identified and promoted four such norms:

- First, a State should not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent of providing competitive advantages to its companies or commercial sectors.
- Second, a State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide service to the public.
- Third, a State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State also should not use CSIRTs to enable online activity that is intended to do harm.
- Fourth, a State should cooperate, in a manner consistent with its domestic and international obligations, with requests for assistance from other States in investigating cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

These four U.S.-promoted norms seek to address specific areas of risk that are of national and/or economic security concern to all States. Although voluntary and non-binding in nature, these norms can serve to define an international standard of behavior to be observed by responsible, like-minded States with the goal of preventing bad actors from engaging in malicious cyber activity. If observed, these measures – which can include measures of self-restraint – can contribute substantially to conflict prevention and stability. Over time, these norms can potentially provide common standards for responsible States to use to identify and respond to behavior that deviates from these norms. As more States commit to observing these norms, they will be increasingly willing to condemn the malicious activities of bad actors and to join together to ensure that there are consequences for those activities.

It is important, however, to distinguish clearly between international law, on the one hand, and voluntary, non-binding norms on the other. These four norms identified by the United States, or

the other peacetime cyber norms recommended in the 2015 UN GGE report, fall squarely in the voluntary, non-binding category. These voluntary, non-binding norms set out standards of expected State behavior that may, in certain circumstances, overlap with standards of behavior that are required as a matter of international law. Such norms are intended to supplement existing international law. They are designed to address certain cyber activities by States that occur outside of the context of armed conflict that are potentially destabilizing. That said, it is possible that if States begin to accept the standards set out in such non-binding norms as legally required and act in conformity with them, such norms could, over time, crystallize into binding customary international law. As a result, States should approach the process of identifying and committing to such non-binding norms with care.

In closing, I wanted to highlight a few points. First, cyberspace may be a relatively new frontier, but State behavior in cyberspace, as in other areas, remains embedded in an existing framework of law, including international law. Second, States have the primary responsibility for identifying how existing legal frameworks apply in cyberspace. Third, States have a responsibility to publicly articulate applicable standards. This is critical to enable an accurate understanding of international law, in the area of cyberspace and beyond. I hope that these remarks have furthered this goal of transparency, and highlighted the important role of international law, and international lawyers, in this important and dynamic area.

Source. https://2009-2017.state.gov/s/l/releases/remarks/264303.htm, accessed 25 July 2018.

B. DOD Law of War Manual

The following is an excerpt from Chapter XVI – Cyber Operations in the *DOD Law of War Manual*, June 2015 (Updated December 2016). The full document can be found at: https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

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]

16.1.1 Cyberspace as a Domain. As a doctrinal matter, DOD has recognized cyberspace as an 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 infrastructures 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 objectives 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 constitutes 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 principle of proportionality 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 this prohibition 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 disruptions, need not be considered in assessing whether an attack is prohibited by the principle of proportionality.[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 principle of proportionality, 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 principle of proportionality in conducting attacks, 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 principle of proportionality.[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 – Prohibition on Attacks Expected to Cause Excessive Incidental Harm).

47 Refer to § 5.7 (Military Objectives).

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

49 Refer to § 5.12 (Proportionality – Prohibition on Attacks Expected to Cause Excessive Incidental Harm).

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: https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190, accessed 25 July 2018.

Intentionally Blank

Appendix B: U.S. Cyberspace Organizations

Appendix B includes:

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

II. **Office of the Director of National Intelligence**
   - **Cyber Threat Intelligence Integration Center (CTIIC)**

III. **Department of Homeland Security**
   - **Cybersecurity and Infrastructure Security Agency (CISA)**

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

V. **Joint Organizations**
   - **Joint Spectrum Center (JSC)**
   - **Joint Communications Support Element (JCSE)**
   - **U.S. Cyber Command (USCYBERCOM)**

VI. **Service Organizations**
   - **Army Cyber Command (ARCYBER)**
   - **Marine Corps Forces Cyber (MARFORCYBER)**
   - **Navy U.S. Fleet Cyber / U.S. TENTH Fleet (FCC-C10F)**
   - **Air Forces Cyber / 24th Air Force**
   - **Coast Guard / Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance & Information Technology (C4ISR&IT)**

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. The 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.

Source: http://www.state.gov/s/cyberissues/, accessed 25 July 2018.

II. Office of the Director of National Intelligence – Cyber Threat Intelligence Integration Center

The Cyber Threat Intelligence Integration Center (CTIIC) is the newest of four multiagency centers under the Office of the Director of National Intelligence (ODNI) integrating intelligence about threats to U.S. national interests. The DNI established CTIIC in 2015, pursuant to a Presidential Memorandum, to produce coordinated IC analysis of foreign cyber threats to U.S. national interests, ensure the information is shared among the federal cyber community, and support the work of operators, analysts, and policymakers with timely intelligence about significant cyber threats and threat actors.

Mission. CTIIC's mission is to build understanding of foreign cyber threats to U.S. national interests to inform decision-making by federal cyber centers, departments and agencies, and policy makers. CTIIC integrates information from the network defense, intelligence, and law enforcement communities; facilitates information-sharing; leads community analysis of cyber threats; and supports interagency planning to develop whole-of-government approaches against cyber adversaries. CTIIC publishes intelligence products that place current cyber threats in context and provide integrated IC assessments of an adversary's capabilities and motivations for using cyber means to achieve its strategic goals.

Responsibilities. The Presidential Memorandum outlined five responsibilities for the Center:

- Provide integrated all-source analysis of intelligence related to foreign cyber threats or to cyber incidents affecting U.S. national interests.
- Support federal cyber centers by providing access to intelligence necessary to carry out their respective missions.
- Oversee development and implementation of intelligence-sharing capabilities to enhance shared situational awareness of intelligence related to foreign cyber threats and incidents.
- Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both U.S. Government and U.S. private sector entities.
- Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

Organizational Structure. The center has three sections focused, respectively, on Awareness, Analysis, and Opportunity:

- Current Intelligence Section builds shared situational awareness of significant foreign cyber threats with context.
- Analysis Integration Section integrates all-source IC analysis of foreign cyber adversaries, threats, and incidents.
- Threat Opportunity Section supports and facilitates interagency development of options leveraging all instruments of national power.

Source: https://www.dni.gov/index.php/ctiic-who-we-are, accessed 25 July 2018.

III. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA)

On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

- CISA leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.
- The name CISA brings recognition to the work being done, improving its ability to engage with partners and stakeholders, and recruit top cybersecurity talent.

What Does CISA Do?

CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

Comprehensive Cyber Protection

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the networks that support the essential operations of federal civilian departments and agencies.

Infrastructure Resilience

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.

Emergency Communications

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.

Source:
https://www.dhs.gov/CISA?utm_source=hp_slideshow&utm_medium=web&utm_campaign=dhsgov, accessed 27 November 2018.

IV. 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 **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.

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.

Cybersecurity. NSA's role in U.S. cybersecurity includes its primary information assurance mission: serving as the National Manager for National Security Systems. National Security Systems include U.S. systems that contain classified information or are otherwise critical to U.S. military or intelligence missions. NSA performs a number of functions that help the Government protect and defend those systems, such as approving standards, techniques, systems, and equipment related to the security of National Security Systems. Additionally, NSA is uniquely positioned to contribute to U.S. cybersecurity because it also has a foreign signals intelligence mission. The two missions complement one another, enhancing the agency's ability to detect and prevent cyber threats. NSA employs experts in signals intelligence, information security, and computer network defense and exploitation. Their work gives NSA end-to-end insights into malicious cyber activity, the activities of hostile foreign powers, and cyber best practices. This expertise is often called on by partners across the Department of Defense and the Intelligence

Community to help the government mitigate threats and secure networks. Finally, NSA works to advance the state of cybersecurity by partnering with industry and academia through research efforts such as the NSA Technology Transfer Program, and the Science of Security Initiative. NSA also helps develop the skills of the next generation of cyber professionals through programs like the NSA Cyber Exercise (NCX), and the Centers of Academic Excellence in Cybersecurity.

Support to the Military. NSA 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. The U.S. government, the military, and many allies rely on NSA's expertise in foreign signals intelligence and information assurance for mission success. NSA's customers range from the highest levels of government, such as the Office of the President, the State Department, and the Joint Chiefs of Staff, all the way down to small teams of warfighters deployed in harm's way. NSA works 24 hours a day, 7 days a week, 365 days a year to ensure that customers receive the critical intelligence and information assurance products and services they need to accomplish their missions and to protect the nation. No single agency can do this alone, which is why NSA partners both inside the United States and with foreign governments.

Source: https://www.nsa.gov/about/ and https://www.nsa.gov/what-we-do/support-the-military/, accessed 25 July 2018.

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

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

The organization includes four deputies and assigned staffs:

Deputy Chief Information Officer for Command, Control, Communications and Computers (C4) and Information Infrastructure Capabilities (IIC) (DCIO C4&IIC). Provides expertise and broad guidance on policy, programmatic, and technical issues relating to C4&IIC to integrate and synchronize DOD-wide communications and infrastructure programs and efforts to achieve and maintain information dominance for the Department.

Deputy Chief Information Officer for Information Enterprise (DCIO IE). Responsible for integrating DOD policy and guidance to create information advantages for Department personnel, organizations, and DOD mission partners. DCIO IE focuses on providing the leadership, strategy, and guidance to adopt a Joint Information Environment based on a single, secure, reliable DOD-wide IT architecture, and key enabling enterprise capabilities.

Deputy Chief Information Officer for Resources and Analysis (DCIO R&A). Responsible for enabling DOD CIO to manage the Department's information technology spending, ensuring that DOD gets the most out of every dollar and that the Warfighter has the tools to do the mission. The Department's IT & cyberspace budget request for fiscal year 2018 was nearly $42 billion, which includes warfighting, command, control, and communications systems; computing services; enterprise services, like collaboration and e-mail; and business systems.

Deputy Chief Information Officer for Cyber Security (DCIO CS). Is also the Chief Information Security Officer (CISO) for DOD and is responsible for ensuring that the Department has a well-defined and well-executed cyber security program. This organization is also responsible for coordinating cyber security standards, policies, and procedures with other federal agencies, coalition partners, and industry.

Source: http://dodcio.defense.gov/ and http://dodcio.defense.gov/About-DoD-CIO/, accessed 25 July 2018.

C. Defense Information Systems Agency (DISA)

Overview: DISA is a combat support agency of the DOD. The agency is composed of more than 8,000 military and civilian employees. 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.

Mission: To conduct DOD Information Network (DODIN) operations for the joint warfighter to enable lethality across all warfighting domains in defense of our Nation.

Vision: To be the trusted provider to connect and protect the warfighter in cyberspace.

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.

DISA's Mission Partner Support: As the 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) DODIN, which maintains command and control (C2) of defensive cyber operations.

DISA delivers hundreds of IT support and service capabilities to our mission partners. These capabilities are captured in our online service catalog, https://www.disa.mil (accessed through each service category link on the top navigation bar). 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), DISA provides direct telecommunications and IT support to the president, vice president, their staff, 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 (JSSC) 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 ten unified combatant commands.

DISA provides DOD IT support through its DOD Enterprise Computing Centers (DECCs), Defense Information Technology Contracting Organization (DITCO) field sites, and special

mission centers, such as the Joint Interoperability Test Command. In addition, DISA operates the DISA Command Center (DCC), 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.

The Mission Partner Engagement Office and Engagement Executives are DISA's principal representatives to the mission partners - receiving their requests, reaching out to them, advocating for their issues, and providing a conduit for their 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 is responsible for achieving and maintaining information superiority through the collection, processing, and dissemination of an uninterrupted flow of information in support of DOD missions. The DOD CIO exercises authority, direction, and control over the director of DISA and organizationally reports to the Secretary of Defense, the principal advisor to the President of the United States on all defense matters and issues.

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, CYBERCOM, 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 CYBERCOM commander who also serves as the initiative's operational sponsor.

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 25 July 2018.

V. Joint Organizations

A. Joint Spectrum Center (JSC)

The Joint Spectrum Center (JSC), a Field Command within the Defense Spectrum Organization (DSO), has leading experts in the areas of spectrum planning, electromagnetic environmental effects (E3), information systems, cyber security, quality assurance, modeling and simulation, and operations to provide complete, spectrum-related services to the Military Departments and Combatant Commands (CCMDs). 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 Branches/Services:

Cyber Security and Quality Assurance (J2) provides information assurance, technical and non-technical cyber operations expertise, and oversight for all DSO spectrum capabilities and developmental efforts. J2 also provides acceptance support for application developments and overall quality assurance processes for the DSO.

Operational Support (J3) provides communications-electronics and electromagnetic battlespace support, and joint spectrum interference resolution support to the CCMDs**.**

Electromagnetic Environmental Effects (E3) Engineering (J5) provides E3 engineering and spectrum supportability (SS) technical support to the Department of Defense Chief Information Officer (DOD/CIO), the Joint Staff, the Services, and other DOD Components through: (1) Management of the DOD E3 Program and Policy Development; (2) Joint Capabilities Acquisition Support; (3) Joint E3 Ordnance Program; (4) DOD Electromagnetic Compatibility Standardization; and (5) E3 and SS Training and Awareness.

Information Systems (J6) provides IT support to the DSO and JSC as the customer advocate for enterprise systems and services to enable mission execution. J6 operates and maintains advanced IT environments supporting deployment and sustainment of spectrum-related software application.

Spectrum Enterprise Services (J7) provides Joint, dynamic, responsive and agile spectrum management enterprise services and capabilities in support of the warfighters' needs and requirements. The Global Electromagnetic Spectrum Information System (GEMSIS) Program Office develops and provides enterprise capabilities and services supporting the DOD.

Applied Engineering Division (J8) provides 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 25 July 2018.

B. Joint Communications Support Element (JCSE)

The Joint Communications Support Element is a subordinate command assigned to the Joint Enabling Capabilities Command and USTRANSCOM. It provides enroute, initial entry, or early entry communications support for up to 40-personnel Joint Task Force (JTF) in support of permissive and non-permissive environments. Additionally, the Element has the requisite skill sets to support larger JTF Headquarters and two Joint Special Operations Task Force (JSOTF) Headquarters – anywhere from 40 to 1500 users.

Mission: On order, JCSE immediately deploys to provide enroute, early entry, scalable C4 support to the Regional Combatant Commands, Special Operations Command, and other agencies as directed; on order, provides additional C4 services within 72 hours to support larger CJTF/CJSOTF Headquarters 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, and one Army Reserve Squadron.

The three active squadrons (1st, 2nd, and 3rd Joint Communications Squadron [JCS]) as well as the HSS and CSD are all headquartered at MacDill AFB, 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 1,500 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 25 July 2018.

C. U.S. Cyber Command (USCYBERCOM)

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 executes its mission through forces drawn from the military service cyber components.

- 2nd Army - U.S. Army Cyber Command (ARCYBER)
- 24th Air Force - Air Forces Cyber (AFCYBER)
- U.S. Tenth Fleet - Fleet Cyber Command (FLTCYBER)
- U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER)

Forces: The USCYBERCOM concept for organization includes 133 Cyber Mission Force (CMF) teams:

- Cyber National Mission Force teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering to defeat them.
- Cyber Combat Mission Force teams conduct military cyber operations in support of combatant commands.
- Cyber Protection Teams defend the DOD information networks, protect priority missions and prepare cyber forces for combat.

USCYBERCOM aligned Cyber Mission Forces in support of the Joint Force. Specifically, CMF teams were focused toward habitually supporting combatant commands under USCYBERCOM's Joint Force Headquarters Cyber construct:

- MARFORCYBER supports U.S. Special Operations Command (USSOCOM)
- ARCYBER supports U.S. Central Command (USCENTCOM), U.S. Africa Command (USAFRICOM) and U.S. Northern Command (USNORTHCOM)
- FLTCYBER supports U.S. Pacific Command (USPACOM) and U.S. Southern Command (USSOUTHCOM)
- AFCYBER supports U.S. European Command (USEUCOM), U.S. Strategic Command (USSTRATCOM), and U.S. Transportation Command (USTRANSCOM)

Source: https://www.cybercom.mil/, accessed 25 July 2018

VI. Service Organizations

A. Army Cyber Command (ARCYBER)

Army Cyber Command is an operational-level Army force reporting directly to Headquarters, Department of the Army (HQDA). The Commander, ARCYBER, exercises operational control over Army forces, as delegated by the Commander, U.S. Cyber Command and is the primary headquarters responsible for conducting cyberspace operations (offensive cyberspace operations, defensive cyberspace operations, and Department of Defense Information Network operations), as directed and authorized on behalf of the Commander, U.S. Strategic Command or the Commander, U.S. Cyber Command. ARCYBER organizes, trains, educates, mans, equips, funds, administers, deploys, and sustains Army cyber forces to conduct cyberspace operations.

Mission. 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.

Vision.

- A force that can aggressively operate and defend our networks, data, and weapons systems
- A force which delivers effects against our adversaries in and through cyberspace to enable commanders' objectives
- A force that designs, builds, and delivers integrated capabilities for the future fight – spanning cyberspace, electronic warfare, and information operations

Organization. Army cyber units include:

U.S. Army Network Enterprise Technology Command (NETCOM) leads global operations for the Army's portion of the Department of Defense Information Networks (DODIN), ensuring freedom of action in cyberspace while denying the same to our adversaries.

1st Information Operations Command (Land) provides Information Operations support to the Army and other Military Forces through:

- Deployable Support Teams
- Opposing forces support
- Reachback planning and analysis
- Specialized training

780th Intelligence Brigade (Cyber) is a Major Subordinate Command under the U.S. Army Intelligence and Security Command, with operational control under the U.S. Army Cyber Command. The brigade conducts cyberspace operations and signals intelligence to create operational effects in and through the cyberspace domain to gain and maintain freedom of action required to support Army and Joint requirements while denying the same to our adversaries.

Source: http://www.arcyber.army.mil/, accessed 25 July 2018.

B. Marine Corps Forces Cyber (MARFORCYBER)

Mission.

1. Commander, Marine Corps Forces Cyberspace Command (COMMARFORCYBERCOM), as the Marine Corps service component commander for the Commander, U.S. Cyber Command, represents Marine Corps capabilities and interests; advises CDRUSCYBERCOM on the proper employment and support of Marine Corps forces; and coordinates deployment, employment, and redeployment planning and execution of attached forces.

2. COMMARFORCYBERCOM enables full spectrum cyberspace operations, to include the planning and direction of Marine Corps Enterprise Network Operations (MCEN Ops), defensive cyberspace operations (DCO) in support of Marine Corps, Joint and Coalition Forces, and the planning and, when authorized, direction of offensive cyberspace operations (OCO) in support of Joint and Coalition Forces, in order to enable freedom of action across all warfighting domains and deny the same to adversarial forces.

3. COMMARFORCYBERCOM has direct operational control of Marine Corps Cyberspace Warfare Group (MCCYWG) and Marine Corps Cyberspace Operations Group (MCCOG) to support mission requirements and tasks.

4. COMMARFORCYBERCOM also serves as Commander, Joint Force Headquarters – Cyber (JFHQ-C) / Marines (JFHQ-C/Marines). JFHQ-C/Marines provides support to Combatant Commands for OCO and, when directed, conducts cyberspace operations through attached cyberspace forces. JFHQ-C/Marines is responsible for the command, control, and tactical direction of attached cyberspace forces.

Subordinate Units.

> **Marine Corps Cyberspace Operations Group (MCCOG)** executes Marine Corps Department of Defense Information Network (DODIN) Operations and Marine Corps DCO in order to enhance freedom of action across warfighting domains, while denying the efforts of adversaries to degrade or disrupt this advantage through cyberspace.
>
> **Marine Corps Cyberspace Warfare Group (MCCYWG)** organizes, trains, equips, provides administrative support, manages readiness of assigned forces, and recommends certification and presentation of Cyber Mission Force (CMF) Teams to USCYBERCOM. The MCCYWG plans and conducts full spectrum cyberspace operations as directed by COMMARFORCYBER in support of service, combatant command, joint, and coalition requirements.

Source: http://www.candp.marines.mil/Organization/Operating-Forces/US-Marine-Corps-Forces-Cyberspace-Command/, accessed 25 July 2018

C. Navy U.S. Fleet Cyber / U.S. TENTH Fleet (FCC-C10F)

Operational – U.S. Fleet Cyber Command/U.S. TENTH Fleet (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.

- U.S. Fleet Cyber Command (FCC) serves as the Navy component command to 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 (C10F) 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.

Fleet Cyber Command

Mission: The mission of Fleet Cyber Command is to plan, coordinate, integrate, synchronize, direct, and conduct the full spectrum of cyberspace operational activities required to ensure freedom of action across all of the Navy's warfighting domains in, through, and from cyberspace, and to deny the same to the Navy's adversaries.

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, DOD, academia, industry, and our foreign partners.

Tenth Fleet

Mission: The mission of Tenth Fleet is to plan, monitor, direct, assess, communicate, coordinate, and execute operations to enable command and control and set the conditions for subordinate success by:

- Serving as the numbered fleet for U.S. Fleet Cyber Command and exercise operational control over U.S. Fleet Cyber Command-assigned forces.
- Directing and delivering desired tactical and operational effects in and through cyberspace, space and the electromagnetic spectrum to Navy commanders worldwide and ensure successful execution of U.S. Fleet Cyber Command-assigned mission areas.

Source: http://www.public.navy.mil/fcc-c10f/Pages/home.aspx and http://www.public.navy.mil/fcc-c10f/Fact%20Sheets/FCC-C10F%20Fact%20Sheet%202014.pdf, accessed 25 July 2018.

D. Air Forces Cyber / 24th Air Force

The command has been assigned three distinct roles and responsibilities. Each has a unique set of authorities and chain of command.

Air Forces Cyber role, the commander presents and employs Air Force cyber forces to support U.S. Cyber Command (USCYBERCOM) for the planning and execution of full-spectrum cyberspace operations across the Air Force Information Network (AFIN), portions of the DOD Information Network (DODIN), and other cyber key terrain as directed.

24th Air Force role, the commander reports directly to the commander of Air Combat Command and is responsible within the Air Force for organizing, training, and equipping ready cyber forces and capabilities in support of joint, coalition and service missions. 24th Air Force also serves as the Cyber Security Service Provider for the Air Force Network (AFNET) and Air Force Network-Secure (AFNET-S), and other designated cyber terrain.

Joint Force Headquarters-Cyber role, the commander is entrusted with leading forces in the planning and, upon the order of the President and/or the Secretary of Defense, the execution of offensive cyberspace operations in support of Combatant Commanders.

More than 5,600 men and women conduct or support 24-hour operations involving cyberspace operations for 24th Air Force, including approximately 3,250 military, 900 civilian and 1,400 contractor personnel. Approximately 1,100 Air Reserve Component personnel came to Air Combat Command (ACC) from existing Air Force Reserve and Air National Guard units associated with the combat communications mission of the 688th Cyberspace Wing, 67th Cyberspace Wing and the Air Force Network Operations.

Organization: The 24th Air Force is comprised of an integrated operations center (OC) (624OC) and two wings (688th and 67th Cyberspace Wings).

> **624th Operations Center,** located at Joint Base San Antonio-Lackland, TX, is aligned under 24th Air Force, Air Combat Command. The unit receives orders and tasks from U.S. Cyber Command and, in turn, tasks 24th AF subordinate units to perform a wide range of cyber missions in support of Air Force and joint force commanders. The 624th OC operates the Cyber Command and Control Mission System weapon system.
>
> **67th Cyberspace Wing,** headquartered at Joint Base San Antonio-Lackland, TX, is the Air Force's newest combat wing, serving as Air Forces Cyber's execution arm for generating, projecting, and sustaining combat power with the employment of the Cyberspace Vulnerability Assessment/Hunter weapon system. Comprised of more than 2,000 Airmen, civilians, and contractors across three operations groups with 26 units at seven locations worldwide, employees conduct network operations, defense, attack, and exploitation in service of the Air Force, combatant commands and national agencies.
>
> **688th Cyberspace Wing,** located at Joint Base San Antonio-Lackland, TX, executes a diverse mission set of cyberspace capability development, test, and assessment; develops and validates cyber tactics; integrates cyber into Air Force Warfare Center training events; employs cyber protection teams to defend priority Department of Defense networks and systems against priority threats; and operates the Air Force cyber and information operations formal training units. The 5th Combat Communications Group, located at Robins AFB, GA, is aligned under the 688th Cyberspace Wing.

Source: https://www.afcyber.af.mil/, accessed 25 July 2018.

E. Coast Guard

Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance & Information Technology (C4ISR&IT)

Mission. To enhance Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Information Technology's value in the performance of Coast Guard missions; accomplished by developing and aligning enterprise strategies, policies, and resource decisions with the Coast Guard Strategic Goals, mandates, and customer requirements.

Goals and Objectives. C4ISR&IT five strategic goals: Cyberspace Operations, Efficient Information Management, Technology and Innovation, Governance and Organizational Excellence.

Goal 1. Cyberspace Operations. Enhance mission effectiveness by preventing C4ISR&IT security incidents, such as cyber attacks and intrusions and enhancing C4ISR&IT security mitigation and recovery. The prevention, mitigation, and recovery objectives support this goal:

1.1 Prevention: Enhance C4ISR&IT cyber security by ensuring that proper safeguards and processes are in place to defend Coast Guard cyberspace and to ensure confidentiality, integrity, availability and privacy of information in alignment with JIE, DOD and DHS policy.

1.1.1 Strengthening Information Security throughout the Coast Guard.

1.1.2 OSC Conversion to DOD Server Hardening Guidelines.

1.1.3 Develop prioritized list of IT Critical Infrastructure and Key Resources.

1.1.4 Build Information Assurance Program.

1.2 Mitigation: Improve the Coast Guard's ability to detect and respond to C4ISR&IT incidents in a timely manner with minimal disruption to systems and the Coast Guard's ability to carry out its missions.

1.2.1 Computer Network Defense (CND) Capabilities.

1.3 Recovery: Deploy and direct appropriate C4ISR&IT resources to rapidly restore Coast Guard systems and data.

1.3.1 Mobile Command Center (MCC) Development.

1.3.2 Contingency SATCOM.

Source – Strategic Plan FY 2015-201: https://www.dcms.uscg.mil/Portals/10/CG-6/FY15-19_C4ISRandIT_Strategic_Plan.pdf?ver=2016-12-05-161842-567, accessed 25 July 2018.

Intentionally Blank

Glossary

Most terms are taken from the *DOD Dictionary of Military and Associated Terms* (as of June 2018). Other cyberspace terms are taken from *Cyber Operations and Cyber Terrorism*, DCSINT Handbook No. 1.02 (15 August 2005) and the U.S. Computer Emergency Readiness Team (US-CERT) web site.

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.

CCDR — Combatant Commander.

CCMD — Combatant Command.

CCMF – Cyber Combat Mission Force.

CERF — Cyber Effects Request Format.

CJCS — Chairman of the Joint Chiefs of Staff.

CMF — Cyber Mission Force.

CMT — Combat Mission Team.

CO-IPE – Cyberspace Operations-Integrated Planning Element

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.

directive authority for cyberspace operations (DACO). The authority to issue orders and directives to all Department of Defense components to execute global Department of Defense information network operations and defensive cyberspace operations internal defensive measures.

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.

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 planning process (JPP) — An orderly, analytical set of logical steps to frame a problem; examine a mission; develop, analyze, and compare alternative courses of action (COAs), select the best COA; and produce a 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-classified Internet Protocol Router Network (NIPRNET) — A global, multi-segment network used by the 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.

ransomware — A type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.

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 (SIPRNET) — 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, *DOD Dictionary of Military and Associated Terms* (Washington, DC: U.S. Joint Chiefs of Staff, as of June 2018), 60.

[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 Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, 16 June 2017), xvi.

[5] JP 5-0, xi.

[6] JP 5-0, xiii.

[7] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: U.S. Joint Chiefs of Staff, 8 June 2018), xii-xiii.

[8] JP 3-12, vii-viii.

[9] JP 3-12, x.

[10] JP 3-12, xvii.

[11] JP 5-0, xxi.

[12] JP 5-0, IV-7.

[13] JP 5-0, IV-6 – 7.

[14] JP 5-0, IV-8.

[15] Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), II, https://www.whitehouse.gov/wp-content/.../2017/12/NSS-Final-12-18-2017-0905.pdf (accessed 9 July 2018).

[16] *National Security Strategy*, 12-13.

[17] *National Security Strategy*, 18-23.

[18] *National Security Strategy*, 32.

[19] *National Security Strategy*, 40-41.

[20] James N. Mattis, *Summary of the National Defense Strategy, Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense), 1, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed 9 July 2018).

[21] *Summary of the National Defense Strategy*, 3.

[22] *Summary of the National Defense Strategy*, 6.

[23] James N. Mattis, *Summary of the 2018 Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, September 2018), 3 – 6, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed 1 November 2018).

[24] JP 5-0, IV-9.

[25] JP 5-0, IV-9.

[26] Department of State, *Recommendations to the President on Protecting American Cyber Interests Through International Engagement* (Washington, DC: Department of State), 1 – 3, https://www.state.gov/s/cyberissues/eo13800/281980.htm (accessed 9 July 2018).

[27] JP 5-0, IV-10.

[28] 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.

[29] 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).

[30] *Cross Domain Synergy in Joint Operations*, 50-51.

[31] U.S. Army, *Cyberspace and Electronic Warfare Operations*, Field Manual 3-12 (Washington DC: Headquarters Department of the Army, 11 April 2017), 1-14.

[32] JP 3-12, I-3.

[33] JP 3-12, I-4 –5.

[34] JP 3-12, I-5.

[35] JP 5-0, IV-14.

[36] JP 3-12, I-11.

[37] JP 3-12, I-12.

[38] Daniel R. Coats, Director of National Intelligence, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence (Washington, DC, 13 February 2018), 4 – 5.

[39] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[40] 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), 4.

[41] "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," linked from *Department of Justice Home Page*, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election (accessed 16 July 2018).

[42] Michael S. Rogers, *Statement Of Admiral Michael S. Rogers Commander United States Cyber Command Before The Senate Committee On Armed Services* (Washington., DC, 27 February 2018), 5 – 6.

[43] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[44] "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 26 May 2017).

[45] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/wanted/cyber/huang-zhenyu/view (accessed 26 May 2017).

[46] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 2.

[47] Michael S. Rogers, *Statement Of Admiral Michael S. Rogers Commander United States Cyber Command Before The Senate Committee On Armed Services, 4 – 5.*

[48] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[49] "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 26 May 2017).

[50] "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 26 May 2017).

[51] 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.

[52] Daniel R. Coats, *2017 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 1.

[53] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[54] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[55] Michael S. Rogers, *Statement Of Admiral Michael S. Rogers Commander United States Cyber Command Before The Senate Committee On Armed Services, 6.*

[56] James R. Clapper, *Statement for the Record Worldwide Cyber Threats*, 4.

[57] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[58] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[59] "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 26 May 2017).

[60] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/wanted/cyber/firas-dardar (accessed 1 April 2016).

[61] "Two Members of Syrian Electronic Army Indicted for Conspiracy," linked from *Department of Justice Home Page*, https://www.justice.gov/usao-edva/pr/two-members-syrian-electronic-army-indicted-conspiracy (accessed 9 July 2018).

[62] Daniel R. Coats, *2018 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 6.

[63] Daniel R. Coats, *2017 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 2.

[64] Daniel R. Coats, *2017 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 2.

[65] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/wanted/cyber/igor-anatolyevich-sushchin (accessed 26 May 2017).

[66] Daniel R. Coats, *2017 Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, 2.

[67] "Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes," linked from *Department of Justice Home Page*, https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible (accessed 9 July 2018).

[68] "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 26 May 2017).

[69] "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 26 May 2017).

[70] 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 26 May 2017).

[71] "Federal Government Contractor in Georgia Charged With Removing and Mailing Classified Materials to a News Outlet" linked from *Department of Justice Home Page,* https://www.justice.gov/opa/pr/federal-government-contractor-georgia-charged-removing-and-mailing-classified-materials-news (accessed 9 July 2018).

[72] 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.

[73] U.S. Computer Emergency Readiness Team, Ransomware, linked from *US-CERT Home Page*, https://www.us-cert.gov/security-publications/Ransomware (accessed 26 May 2017).

[74] U.S. Army, *Cyber Operations and Cyber Terrorism*, II-8 – 11.

[75] JP 5-0, IV-15 – 16.

[76] JP 3-12, IV-2 – 3.

[77] JP 5-0, IV-16.

[78] JP 3-12, II-9 – 10.

[79] 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.

[80] JP 3-12, II-2 – 5.

[81] JP 3-12, II-3.

[82] JP 3-12, II-5 – 7.

[83] JP 5-0, IV-17.

[84] JP 3-12, IV-23 – 24.

[85] JP 5-0, IV-17.

[86] JP 3-12, IV-7.

[87] JP 3-12, IV-9.

[88] JP 3-12, IV-20.

[89] JP 5-0, IV-17.

[90] JP 3-12, IV-1.

[91] JP 5-0, xiii.

[92] JP 5-0, V-2.

[93] JP 5-0, V-4 – 49.

[94] JP 5-0, V-2.

[95] JP 3-12, IV-1.

[96] JP 5-0, V-4.

[97] FM 3-12, 3-14 – 15.

[98] JP 5-0, V-4.

[99] FM 3-12, 3-15 – 16.

[100] JP 5-0, V-20.

[101] FM 3-12, 3-16 – 17.

[102] JP 5-0, V-31 – 46.

[103] FM 3-12, 3-17 – 20.

[104] JP 5-0, VI-49 – 50.

[105] JP 3-12, 3-20.

[106] 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.

[107] JP 3-12, II-10 – 11.

[108] JP 3-12, IV-6.

[109] *Cross Domain Synergy in Joint Operations*, 55-56.

[110] JP 3-12, IV-18.

[111] FM 3-12, B-2

[112] FM 3-12, B-3 – 6.

[113] JP 5-0, IV-21 – 23.

[114] JP 3-12, x.

[115] JP 3-12, I-2.

[116] JP 3-12, I-12.

[117] JP 3-12, IV-3.

[118] JP 3-12, IV-10.

[119] FM 3-12, C-1 – 2.

[120] FM 3-12, C-4.

[121] JP 5-0, xvii.

[122] U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication 3-33 (Washington, DC: U.S. Joint Chiefs of Staff, 31 January 2018), IX-8.

[123] U.S. Joint Chiefs of Staff, *Planners Handbook for Operational Design* (Washington, DC: U.S. Joint Chiefs of Staff, 7 October 2011), IX-2 – 3.

[124] JP 3-12, IV-1 – 2.

[125] JP 3-12, III-11.

[126] JP 3-12, III-3.

[127] JP 3-12, III-7.

[128] JP 3-12, IV-17.

[129] JP 3-12, IV-11 – 17.

[130] JP 3-12, III-6.

[131] U.S. Cyber Command, *All Cyber Mission Force Teams Achieve Initial Operating Capability*, (Ft. Meade, MD: U.S. Cyber Command News Release, 24 Oct 2016), 1-3.

[132] JP 3-12, IV-14.

[133] JP 3-12, IV-19 – 20.

[134] JP 3-12, IV-8 – 10.

[135] JP 3-12, IV-21.

[136] Barrack Obama, President of the USA, *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, 13 February 2015, Stanford University, Stanford, CA.

[137] *Summary of the National Defense Strategy*, 4.

[138] U.S. Joint Chiefs of Staff, *Homeland Defense*, Joint Publication 3-27 (Washington, DC: U.S. Joint Chiefs of Staff, 10 April 2018), vii – viii.

[139] JP 3-27, I-1 – 3.

[140] Critical Infrastructure Sectors, linked from the *Department of Homeland Security Home Page*, https://www.dhs.gov/critical-infrastructure-sectors (accessed 26 May 2017).

[141] DOD Protected Critical Infrastructure Program, linked from *Under Secretary of Defense for Policy Home Page*, http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram.aspx (accessed 26 May 2017).

[142] *Department of Defense Cyber Strategy* (Washington, DC: Department of Defense, April 2015), 14.

[143] JP 3-27, II-3.

[144] JP 3-27, II-13.

[145] JP 3-27, II-8.

[146] JP 3-27, II-12.

[147] Admiral Michael S. Rogers, *Statement Before the Senate Armed Services Committee* (27 February 2018), 12.

[148] Michael S. Rogers, *Statement Of Admiral Michael S. Rogers Commander United States Cyber Command Before The Senate Committee On Armed Services* (Washington, DC: 7 May 2017), 7 – 8.

[149] JP 3-12, I-13 – 14.

[150] *DOD Cyber Strategy*, 23.

[151] *DOD Cyber Strategy*, 2.

[152] JP 3-12, III-2.

[153] JP 3-12, I-12 – 13.

[154] *DOD Cyber Strategy*, 10-11.

[155] *DOD Cyber Strategy*, 22.

[156] Admiral Michael S. Rogers, *Statement Before the Senate Armed Services Committee* (27 February 2018), 16.

[157] *DOD Cyber Strategy*, 22-23.

[158] Department of Defense, Policy Memorandum 16-002, *Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DOD Information Networks, Software, and Hardware for State Cyberspace Activities*, (Washington, DC: Department of Defense, 24 May 2016 / Extension Memo 1 March 2018), 1 – 2.

[159] Department of Defense, Directive-Type Memorandum (DTM) 17-007 – *Interim Policy and Guidance for Defense Support to Cyber Incident Response*, (Washington, DC: Department of Defense, 21 June 2017), 2 – 3.

[160] JP 3-12, III-10 – 11.

[161] JP 3-12, III-11.

[162] *Cross Domain Synergy in Joint Operations*, 4.

[163] E. Lincoln Bonner III, Cyber Power in 21st-Century Joint Warfare, *Joint Force Quarterly* 74 (3rd Quarter 2014): 105.

[164] *Cross Domain Synergy in Joint Operations*, 4.

[165] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 104-105.

[166] JP 6-0, ix.

[167] JP 6-0, I-7.

[168] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 106.

[169] Cyber Power in 21st-Century Joint Warfare, JFQ 74, 105.


THE UNITED STATES ARMY WAR COLLEGE


U.S.ARMY
STRENGTH
and WISDOM


CENTER for
STRATEGIC
LEADERSHIP
CSL