United States Army War College


# Strategic Cyberspace Operations Guide

## 28 September 2022

Assistant Professor Benjamin C. Leitzel
Assistant Professor Gregory D. Hillebrand

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.

**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 Professor Benjamin Leitzel and Professor Gregory D. Hillebrand.

4. Changes from the previous volume (dated 1 August 2021) include the 2022 Annual Threat Assessment of the US Intelligence Community, the US Cyber Command Commander's Congressional Testimony, the Department of Justice's Comprehensive Cyber Review, and the Department of State's Bureau of Cyberspace and Digital Policy (CDP).

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

*"While we are having success deterring conventional aggression against the United States, our adversaries are increasingly resorting to malign activity in less traditional areas to undermine our security, … There is perhaps no area where this is more true than in the cyber domain."*

—Dr. Mark T. Esper,
Secretary of Defense[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) provide strategic direction by communicating broad objectives 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 (JS), Combatant Commands (CCMDs), Services, joint forces, combat support agencies (CSAs), and other DOD agencies. It provides purpose and focus to the planning for employment of military force. Strategic direction identifies a desired military objective or end state, national-level planning assumptions, and national-level limitations.[4] At the operational level, joint planning translates national level guidance into specific activities aimed at achieving strategic and operational objectives and attaining the military end state. Plans translate the broad intent provided by a strategy into operations; successful operations achieve the strategy's objectives.[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 the command's broad, long-range objectives that

---

[1] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy," linked from *United States Department of Defense Home Page*, 20 September 2019, https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-DODs-increased-cyber-offensive-strategy/.

[2] U.S. Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: U.S. Joint Chiefs of Staff, as of January 2021), 55.

[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, 1 December 2020), II-5.

[5] JP 5-0, xii.

contribute to national security. The command strategy provides the link between national strategic guidance and joint planning.[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]

[6] JP 5-0, xvii.

[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.

# Chapter 2: Design

## I. Operational Design

1. Joint Publication 5-0, *Joint Planning*, describes operational design and the joint planning process (JPP). Operational art and operational design enable understanding. Understanding is more than just knowledge of the capabilities and capacities of the relevant actors or the scope and nature of the operational environment (OE); it provides context for decision making and how the many facets of the problem are likely to interact, enabling commanders and planners to identify hazards, threats, consequences, opportunities, and risk. Operational art is the cognitive approach used by commanders and staffs – supported by their skill, knowledge, experience, creativity, and judgment – to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, means, and risks. Operational art is inherent in all aspects of operational design. Operational design is the analytical framework that underpins planning. Operational design supports commanders and planners in organizing and understanding the OE as a complex interactive system. Operational design is interwoven with the planning process to fill in gaps in guidance and information and provide a framework in which to plan, enabling planners to address the complexity of the OE, support mission analysis and COA development, and develop a concept of operations with the highest likelihood of success.[11]

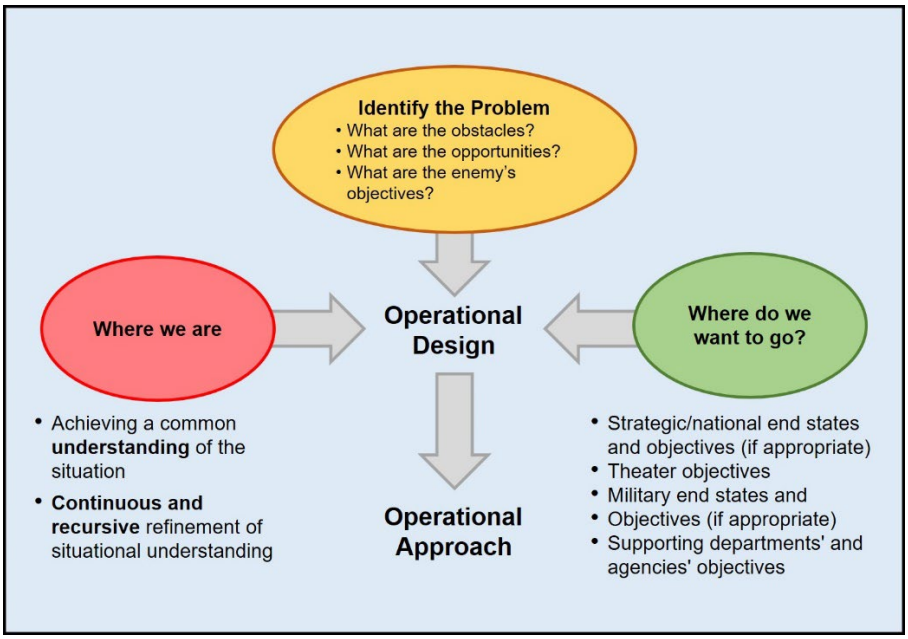


**Figure III-3: Developing the Operational Approach**[12]

a. Operational design requires recurring touch points between the commander and staff in developing an understanding of the strategic environment and OE, higher-level guidance, defining the problem to be solved, and developing an operational approach. The components have characteristics that exist outside of each other and are not

[11] JP 5-0, IV-1.

[12] JP 5-0, III-10.

necessarily sequential. However, an understanding of the OE and problem must be established prior to developing operational approaches and is critical in conducting mission analysis and in providing planning guidance. As commanders and staffs develop their operational approach, they account for how information impacts the OE and the inherent informational aspects of activities. In doing so, joint force planners consider how information is used by, and affects the behavior of friendly, neutral, and adversarial audiences across the competition continuum.

b. The general methodology in operational design is:

(1) Understand the strategic direction and guidance.

(2) Understand the strategic environment (e.g., policies, diplomacy, and politics) and the related contested environments.

(3) Understand the OE and relevant contested environments.

(4) Define the problem (create a shared understanding; planning with uncertainty).

(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.

c. Iteration and reexamination of earlier work is essential to identify how later decisions affect earlier assumptions and to fill in gaps identified during the process.[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 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 objectives (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 March 2021, President Biden issued the Interim National Security Strategic Guidance. The White House issued this interim guidance to convey President Biden's vision for how America will engage with the world, and to provide guidance for departments and agencies to align their actions as the Administration begins work on a National Security Strategy.[15]

---

[13] JP 5-0, IV-2 – 3.

[14] JP 5-0, IV-4.

[15] Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), II, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

a. In foreign policy and national security, just as in domestic policy, we have to chart a new course:

(1) Many of the biggest threats we face respect no borders or walls, and must be met with collective action. Pandemics and other biological risks, the escalating climate crisis, cyber and digital threats, international economic disruptions, protracted humanitarian crises, violent extremism and terrorism, and the proliferation of nuclear weapons and other weapons of mass destruction all pose profound and, in some cases, existential dangers.

(2) Democracies across the globe, including our own, are increasingly under siege. Democratic nations are also increasingly challenged from outside by antagonistic authoritarian powers. Anti-democratic forces use misinformation, disinformation, and weaponized corruption to exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance.

(3) The distribution of power across the world is changing, creating new threats. China, in particular, has rapidly become more assertive. Russia remains determined to enhance its global influence and play a disruptive role on the world stage. Regional actors like Iran and North Korea continue to pursue game-changing capabilities and technologies, while threatening U.S. allies and partners and challenging regional stability. We also face challenges within countries whose governance is fragile, and from influential non-state actors that have the ability to disrupt American interests. Terrorism and violent extremism, both domestic and international, remain significant threats.

(4) The alliances, institutions, agreements, and norms underwriting the international order the United States helped to establish are being tested. Together with our allies and partners, we can modernize the architecture of international cooperation for the challenges of this century, from cyber threats to climate change, corruption, and digital authoritarianism.

(5) Running beneath many of these broad trends is a revolution in technology that poses both peril and promise. Rapid changes in technology will shape every aspect of our lives and our national interests, but the direction and consequences of the technological revolution remain unsettled. Emerging technologies remain largely ungoverned by laws or norms designed to center rights and democratic values, foster cooperation, establish guardrails against misuse or malign action, and reduce uncertainty and manage the risk that competition will lead to conflict.[16]

b. Ensuring our national security requires us to:

(1) Defend and nurture the underlying sources of American strength, including our people, our economy, our national defense, and our democracy at home.

(2) Promote a favorable distribution of power to deter and prevent adversaries from directly threatening the United States and our allies, inhibiting access to the global commons, or dominating key regions.

---

[16] Interim *National Security Strategic Guidance*, 7-8.

(3) Lead and sustain a stable and open international system, underwritten by strong democratic alliances, partnerships, multilateral institutions, and rules.[17]

c. As we bolster our scientific and technological base, we will make cybersecurity a top priority, strengthening our capability, readiness, and resilience in cyberspace. We will:

(1) Elevate cybersecurity as an imperative across the government.

(2) Work together to manage and share risk and encourage collaboration between the private sector and the government at all levels in order to build a safe and secure online environment for all Americans.

(3) Expand our investments in the infrastructure and people we need to effectively defend the nation against malicious cyber activity, providing opportunities to Americans of diverse backgrounds as we build an unmatched talent base.

(4) Renew our commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace.

(5) Hold actors accountable for destructive, disruptive, or otherwise destabilizing malicious cyber activity, and respond swiftly and proportionately to cyberattacks by imposing substantial costs through cyber and noncyber means.[18]

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.[19]

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.[20]

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

---

[17] *Interim National Security Strategic Guidance*, 9.

[18] *Interim National Security Strategic Guidance*, 18.

[19] James N. Mattis, *Summary of the 2018 Department of Defense National Defense Strategy of the United States of America*, (Washington, DC: Department of Defense, September 2018), 1, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

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

advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.[21]

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[22]

## 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, economic, or commercial ramifications that may impact third-party willingness to support US activities including, but not limited to, access, basing, and overflight decisions)?

c. What are the current national strategic objectives of the United States Government (USG)? Are the objectives expected to be long lasting or short-term only? Could they result in unintended consequences (e.g., is there sufficient time to develop strong

---

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

[22] James N. Mattis, *Summary Department of Defense Cyber Strategy 2018* (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.

controls so that weapons provided to a nation will not be used for unintended purposes)?[23]

2. Within the OE, strategic-level considerations may include global factors such as international law; the capability of adversary/enemy diplomatic, information, military, and economic activities to influence domestic and world opinion; adversary and friendly organizations and institutions; and the capability and availability of national and commercial transportation, space capabilities, and information technology.[24]

3. **Policy on Deterring Adversaries and Better Protecting the American People from Cyber Threats**. In 2017, 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.[25]

## 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

---

[23] JP 5-0, IV-5.

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

[25] Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats* (Washington, DC: Department of State, 31 May 2018), 1 – 3, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

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.[26]

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.[27]

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"[28] 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.

---

[26] JP 5-0, IV-6.

[27] U.S. Joint Chiefs of Staff, *Cross Domain Synergy in Joint Operations Planner's Guide*, (Washington, DC: U.S. Joint Chiefs of Staff, 14 January 2016), 49-50.

[28] 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).

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.[29]

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

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

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.[30]

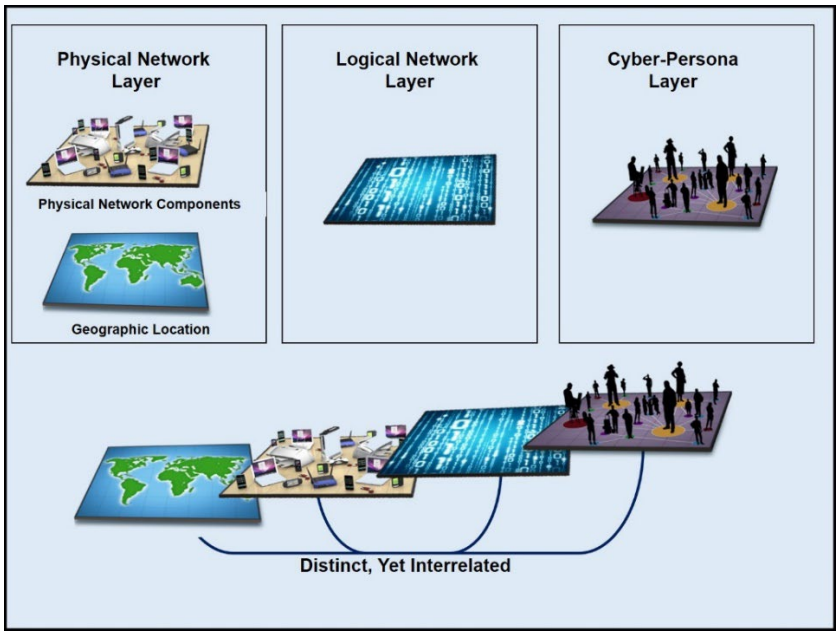


**Figure 2-2. The Three Layers of Cyberspace**[31]

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

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

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.[32]

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., Non-classified Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS)] 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.[33]

## 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 that are 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 of current conditions and how inertia in the OE can be leveraged to enable the desired conditions to achieve the objectives.[34] The commander faces a

---

[32] JP 3-12, I-4 – 5.

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

[34] JP 5-0, IV-11.

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.[35]

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.

---

[35] JP 3-12, I-11 – 12.

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.[36]

4. **Assessment of Cyberspace Threats**. In April 2021, the Director of National Intelligence (DNI) stated "Cyber threats from nation states and their surrogates will remain acute. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. Although an increasing number of countries and nonstate actors have these capabilities, we remain most concerned about Russia, China, Iran, and North Korea. Many skilled foreign cybercriminals targeting the United States maintain mutually beneficial relationships with these and other countries that offer them safe haven or benefit from their activity."[37]

a. **Transnational Threats**. States' increasing use of cyber operations as a tool of national power, including increasing use by militaries around the world, raises the prospect of more destructive and disruptive cyber activity. As states attempt more aggressive cyber operations, they are more likely to affect civilian populations and to embolden other states that seek similar outcomes.

---

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

[37] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, (Washington, DC: Office of the Director of National Intelligence, 9 April 2021), 20, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

(1) Authoritarian and illiberal regimes around the world will increasingly exploit digital tools to surveil their citizens, control free expression, and censor and manipulate information to maintain control over their populations. Such regimes are increasingly conducting cyber intrusions that affect citizens beyond their borders – such as hacking journalists and religious minorities or attacking tools that allow free speech online – as part of their broader efforts to surveil and influence foreign populations. Democracies will continue to debate how to protect privacy and civil liberties as they confront domestic security threats and contend with the perception that free speech may be constrained by major technology companies. Authoritarian and illiberal regimes, meanwhile, probably will point to democracies' embrace of these tools to justify their own repressive programs at home and malign influence abroad.

(2) During the last decade, state sponsored hackers have compromised software and IT service supply chains, helping them conduct operations – espionage, sabotage, and potentially prepositioning for warfighting.[38]

b. **China**. In February 2022, the DNI assessed that China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally.

(1) China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems.

(2) China leads the world in applying surveillance and censorship to monitor its population and repress dissent, particularly among minorities. Beijing conducts cyber intrusions that affect U.S. and non-U.S. citizens beyond its borders – such as hacking journalists – to counter perceived threats to the CCP and tailor influence efforts.

(3) China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.[39]

c. **Russia**. The DNI assessed that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions, as well as a deterrence and military tool.

(1) Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising

---

[38] *Annual Threat Assessment of the US Intelligence Community*, (2021), 20-21.

[39] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, (Washington, DC: Office of the Director of National Intelligence, 7 February 2022), 8, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.

(2) Russia is also using cyber operations to attack entities it sees as working to undermine its interests or threaten the stability of the Russian Government. Russia attempts to hack journalists and organizations worldwide that investigate Russian Government activity and in several instances, has leaked their information.

(3) Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities, and it is developing, testing, and fielding an array of nondestructive and destructive counterspace weapons – including jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based antisatellite (ASAT) capabilities – to target U.S. and allied satellites.[40]

d. **Iran**. The DNI stated that Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data. Iran's opportunistic approach to cyber attacks makes critical infrastructure owners in the United States susceptible to being targeted by Tehran, especially when Tehran believes it must demonstrate that it can push back against the United States in other domains. Recent attacks on Israeli and U.S. targets show that Iran is more willing than before to target countries with stronger capabilities.

(1) Iran was responsible for multiple cyber attacks between April and July 2020 against Israeli water facilities. Iran's successful disruption of critical infrastructure in Israel – also a superior cyber power compared with Iran – reflects its growing willingness to take risks when it believes retaliation is justified.[41]

e. **North Korea**. The DNI assessed that North Korea's poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action.

(1) Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States.

(2) Cyber actors linked to North Korea have conducted espionage efforts against a range of organizations, including media, academia, defense companies, and governments, in multiple countries.[42]

f. **Terrorists**. The DNI testified that "terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects – defacing websites or

---

[40] *Annual Threat Assessment of the US Intelligence Community*, (2022), 12-13.

[41] *Annual Threat Assessment of the US Intelligence Community*, (2022), 15.

[42] *Annual Threat Assessment of the US Intelligence Community*, (2022), 17.

executing denial-of-service attacks against poorly protected networks – with little to no warning."[43]

g. **Cyber Criminals**. Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide. These criminals are driven by the promise of large profits, reliable safe havens from which to operate, and a decreasing technical barrier to entry for new actors.

(1) Many major transnational cybercrime groups have diversified business models that engage in direct wire-transfer fraud from victims, or use other forms of extortion alongside or in place of ransomware. In 2020, business-e-mail compromise, identity theft, spoofing, and other extortion schemes ranked among the top five most costly cybercriminal schemes.

(2) U.S. Government entities, businesses, and other organizations face a diverse range of ransomware threats. Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up.[44]

h. **Insider Threats**. While much of our intelligence is focused on external threats, the U.S. must be aware of threats from within.

(1) In 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 SIPRNET.[45]

(2) In 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.[46]

(3) In 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

---

[43] Daniel R. Coats, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Committee*, (Washington, DC: Senate Select Committee on Intelligence, 29 January 2019), 6.

[44] *Annual Threat Assessment of the US Intelligence Community*, (2022), 24.

[45] "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/.

[46] "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.

intent of allowing foreign nations to gain access to that information or to damage essential systems.[47]

(4) In 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.[48]

(5) In 2018, a former U.S. Air Force intelligence specialist has been charged with betraying her oath to protect and defend the United States by delivering sensitive national defense information to the Iranian government, according to an indictment unsealed by the Department of Justice. Monica Witt, who served in the Air Force from 1997 through 2008 and then with a cleared defense contractor until 2010, is charged alongside four Iranians who allegedly used information provided by Witt in a cyber campaign to target and compromise other U.S. security personnel.[49]

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

a. **Brute-Force Attack**. In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time.

(1) **Password-Spray Attack**. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

(2) **Email** applications are also targeted. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud; (2) subsequently download user mail to locally stored email files; (3) identify the entire company's email address list; and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.[50]

b. **Cryptojacking** occurs when malicious cyber actors effectively hijack the processing power of the victim devices and systems by exploiting vulnerabilities – in webpages, software, and operating systems – to illicitly install cryptomining software on victim

---

[47] Former U.S. Nuclear Regulatory Commission Employee Pleads Guilty to Attempted Spear-Phishing Cyber-Attack on Department of Energy Computers, linked from *Department of Justice Home Page*, https://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear-phishing-cyber.

[48] "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.

[49] "Wanted by the FBI," linked from the *FBI Home Page*, https://www.fbi.gov/news/stories/monica-witt-charged-with-espionage-iran-cyber-actors-indicted-021319.

[50] Alert (TA18-086A) Brute Force Attacks Conducted by Cyber Actors, linked from *Cybersecurity and Infrastructure Security Agency Home Page*, https://us-cert.cisa.gov/ncas/alerts/TA18-086A.

devices and systems. With the cryptomining software installed, the malicious cyber actors earn cryptocurrency.

(1) **Cryptocurrency** is a digital currency used as a medium of exchange, similar to other currencies. Unlike other currencies, cryptocurrency operates independently of a central bank and uses encryption techniques and blockchain technology to secure and verify transactions.

(2) **Cryptomining** (cryptocurrency mining) is the way in which cryptocurrency is earned. Individuals mine cryptocurrency by using cryptomining software to solve complex mathematical problems involved in validating transactions. Each solved equation verifies a transaction and earns a reward paid out in the cryptocurrency.[51]

c. **Denial-of-Service (DoS)** is an attack that occurs when a malicious cyber threat actor prevents legitimate users from accessing information systems, devices, or other network resources. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

d. **Distributed Denial-of-Service (DDoS)** attacks occur when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet – a group of hijacked internet-connected devices to carry out large scale attacks.

(1) **Command and Control**. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

(2) **Botnets** – made up of compromised devices – may also be rented out to other potential attackers. Often the botnet is made available to "attack-for-hire" services, which allow unskilled users to launch DDoS attacks.

(3) **Internet of Things (IoT)**. DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things. IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners' knowledge.[52]

---

[51] Security Tip (ST18-002) Defending Against Illicit Cryptocurrency Mining Activity, linked from *Cybersecurity and Infrastructure Security Agency Home Page*, https://us-cert.cisa.gov/ncas/tips/ST18-002.

[52] Security Tip (ST04-015) Understanding Denial-of-Service Attacks, linked from *Cybersecurity and Infrastructure Security Agency Home Page*, https://us-cert.cisa.gov/ncas/tips/ST04-015.

e. **Malicious Code** is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include: viruses, worms, and Trojan horses.

(1) **Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.

(2) **Worms** are a type of virus that self-propagates from computer to computer. Its functionality is to use all of your computer's resources, which can cause your computer to stop responding.

(3) **Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program. It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software. Instead the program is performing malicious actions on your computer.

(4) **Malicious Data Files** are non-executable files – such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file – that exploit weaknesses in the software program used to open it. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing the files via email, social media, and websites.[53]

f. **Ransomware** is a type of malicious software cyber actors use to deny access to systems or data. It is frequently delivered through spearphishing emails and targets critical data and systems for the purpose of extortion. Ransomware often attempts to spread to shared storage drives and other accessible systems. The malicious cyber actor holds systems or data hostage until a ransom is paid. If payment is received, the cyber actor will purportedly provide an avenue for the victim to regain access to the system or data. If the demands are not met, the system or encrypted data remains unavailable, or the data may be deleted.[54]

g. A **Rootkit** is a piece of software that can be installed and hidden on your computer without your knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of a vulnerability on your computer or has convinced you to download it. Rootkits are not necessarily malicious, but they may hide malicious activities. If a Rootkit has been installed, the user may not be aware that their computer has been compromised, and traditional anti-virus software may not be able to detect the malicious programs. Attackers may be able to access information, monitor your actions, modify programs, or perform other functions on your computer without being detected. Attackers are also creating more sophisticated programs that update themselves so that they are even harder to detect.[55]

---

[53] Security Tip (ST18-004) Protecting Against Malicious Code, linked from *Cybersecurity and Infrastructure Security Agency Home Page,* https://us-cert.cisa.gov/ncas/tips/ST18-271.

[54] Department of Homeland Security, *Ransomware, What it is and What to do about it*, (Washington, DC, Department of Homeland Security), https://us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf.

[55] Security Tip (ST06-001) Understanding Hidden Threats: Rootkits and Botnets, linked from *Cybersecurity and Infrastructure Security Agency Home Page,* https://us-cert.cisa.gov/ncas/tips/ST06-001.

h. **Social Engineering Attacks**. An attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

(1) **Phishing** is a form of social engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy organization. Phishing emails are crafted to appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

(2) **Vishing** is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed.

(3) **Smishing** is a form of social engineering that exploits Short Message Service (SMS) or text messages. Text messages can contain links to such things as webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.[56]

i. **Spyware** collects information from a computing system without user consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information. The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.

(1) **Key Loggers** capture keyboard events and record the keystroke data before it is sent to the intended application for processing. Like most other spyware capture technologies, software based keyloggers can turn their capture on or off based on keywords or events.

(2) **Network Traffic** is another valuable source of data. Data commonly extracted from network captures includes user names, passwords, email messages, and web content. In some cases, entire files can be extracted and reconstructed from the captured streams.[57]

j. **Wireless Threats**. A wireless-enabled laptop can expose the user to a number of security threats.

(1) **Evil Twin Attacks**. The attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus

---

[56] Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks, linked from *Cybersecurity and Infrastructure Security Agency Home Page,* https://us-cert.cisa.gov/ncas/tips/ST04-014.

[57] Department of Homeland Security, *Spyware*, (Washington, DC, Department of Homeland Security), https://us-cert.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf.

signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet.

(2) **Wireless Sniffing**. Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

(3) **Peer-to-Peer Connections**. Many laptop computers can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections. An attacker with a network card configured for ad hoc mode and using the same settings as the victim's computer may gain unauthorized access to sensitive files. An unsecured wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.[58]

## 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.[59]

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.[60]

---

[58] Department of Homeland Security, *Using Wireless Technology Securely*, Washington, DC, Department of Homeland Security), https://us-cert.cisa.gov/sites/default/files/publications/Wireless-Security.pdf.

[59] JP 5-0, IV-13 – 14.

[60] JP 3-12, IV-2 – 3.

## 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 provides the foundation for the commander's planning guidance to the staff and other partners by providing the commander's visualization of how the joint force's operations will 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.[61]

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).[62]

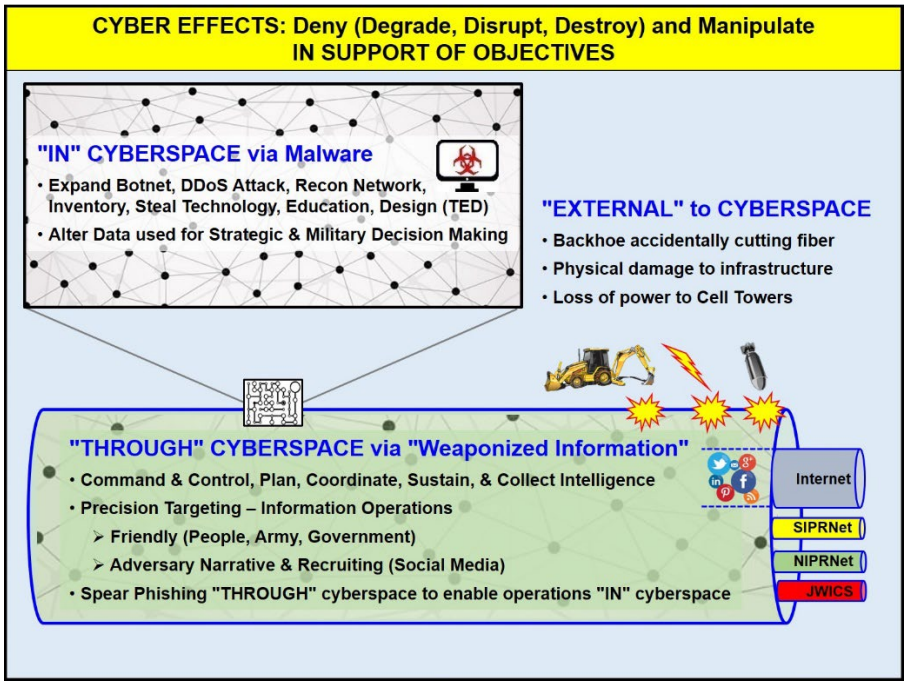


**Figure 2-3: Operations In, Through, and External to Cyberspace**

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

[61] JP 5-0, IV-14 – 15.

[62] JP 3-12, II-9 – 10.

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.[63]

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

[63] 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.

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.[64]

[64] JP 3-12, II-2 – 5.

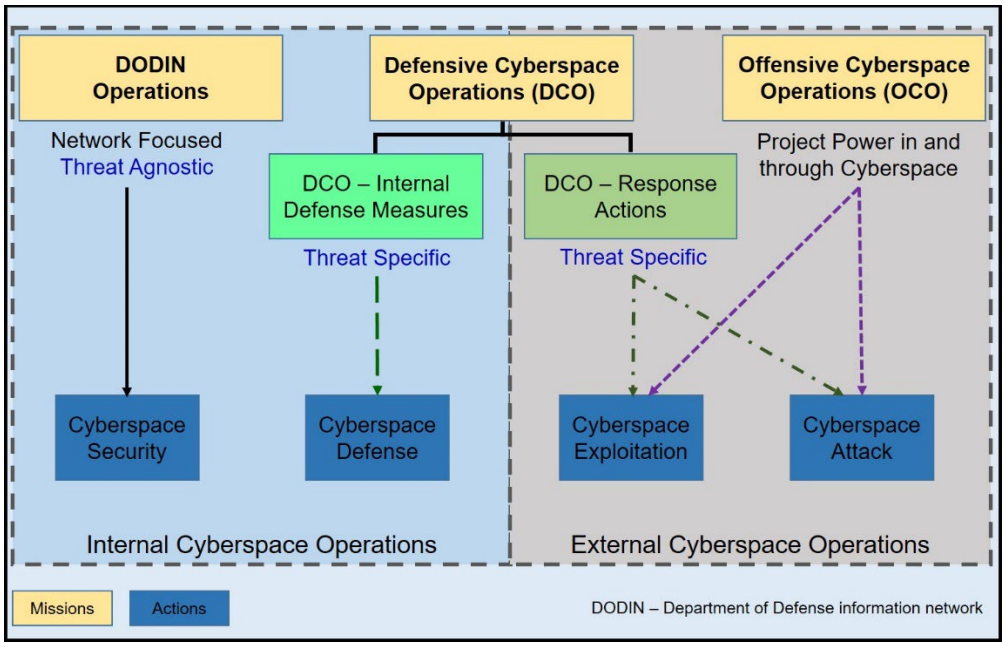


**Figure 2-4: Cyberspace Missions and Actions**[65]

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,

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

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.[66]

## 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 military and civilian leaders a template and warning for the decisions in advance and helps facilitate collaboration with interagency partners and allies to develop alternatives and exploit opportunities short of escalation. The decision matrix also identifies the expected indicators needed in support of operation assessment and intelligence requirements and collection plans.[67]

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.[68]

## 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 suitable. The commander adjusts the operational approach based on feedback from the formal and informal discussions at all levels of command and other information.[69]

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.[70]

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

---

[66] JP 3-12, II-5 – 7.

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

[68] JP 3-12, IV-23 – 24.

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

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

a result, engaging targets in and through cyberspace requires close coordination within DOD and with interagency and multinational partners.[71]

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.[72]

## 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 issues planning guidance, as appropriate, to help focus the staff efforts.[73]

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.[74]

---

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

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

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

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

**Intentionally Blank**

# Chapter 3: Planning

## I. Joint Planning Process (JPP)

1. **Planning**. Plans translate the broad intent provided by a strategy into operations; successful operations achieve the strategy's objectives. The effects of operations, successful or otherwise, change the strategic environment and the operational environment (OE). To maintain a competitive advantage, the joint force should constantly evaluate effects and objectives, align them with strategic objectives, and verify that they are still relevant and feasible. Joint forces, through their assessments, identify when their actions begin to negatively affect the OE and change their operations and activities to create the desired effects and better align actions and objectives.[75]

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.[76]

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).[77]

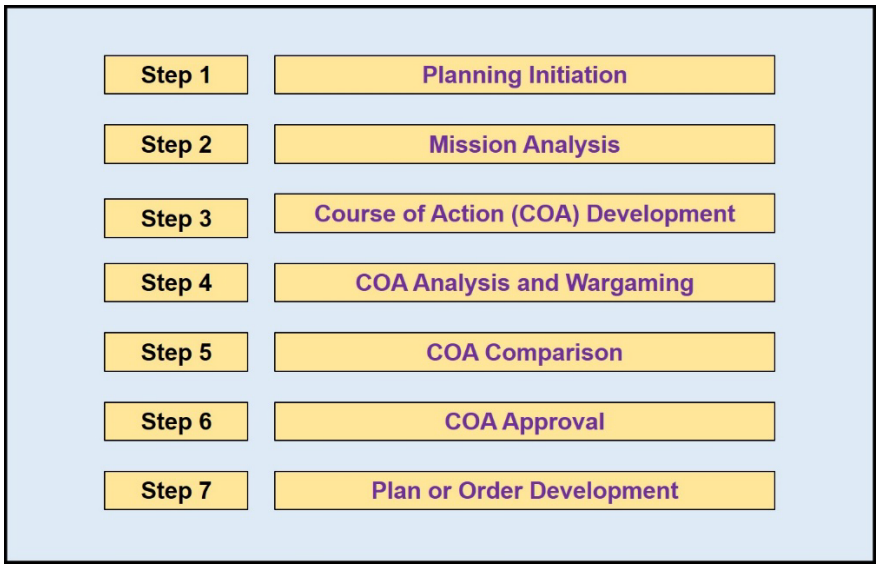


**Figure 3-1: Joint Planning Process**[78]

---

[75] JP 5-0, I-2.

[76] JP 5-0, III-4.

[77] JP 5-0, III-10.

[78] JP 5-0, III-11.

## 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.[79]

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.[80]

(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.[81]

b. **Mission Analysis (Step 2)**. The commander and staff develop a restated mission statement that 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.[82]

(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.

---

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

[80] JP 5-0, III-12.

[81] FM 3-12, 3-14 – 15.

[82] JP 5-0, III-13.

- Cyberspace limitations and constraints.
- Cyberspace assumptions.
- Updated CO running estimate.[83]

c. **Course of Action (COA) Development (Step 3)**. A COA is a potential way (solution, method) to accomplish the assigned mission. Staffs develop multiple COAs to provide commanders with options to attain 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. All COAs must be suitable, feasible, acceptable, distinguishable, and complete. Planners can vary COAs by adjusting the use of joint force capabilities by employing the capabilities in combination for effectiveness making use of the information environment (including cyberspace) and the electromagnetic spectrum throughout the OE.[84]

(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.[85]

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 enable the commander and staff to tentatively evaluate COA validity 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. COA analysis is a valuable use of time that ensures COAs are valid. Wargaming is a primary means for this analysis. Once COA analysis is complete, the staff determines which COA performs best against the established evaluation criteria. The commander reviews the criteria list and adds or deletes, as required. COAs are not compared with each other within any one criterion, but rather, they are individually evaluated against the criteria that are established by the staff and commander. Their individual performances are then compared to enable the staff to recommend a preferred COA to the commander.

Finally, the staff briefs the commander on the COA comparison and the analysis and wargaming results, including a review of important supporting information. The

---

[83] FM 3-12, 3-15 – 16.

[84] JP 5-0, III-32.

[85] FM 3-12, 3-16 – 17.

commander, upon receiving the staff's recommendation, combines personal analysis with the staff recommendation, resulting in a selected COA.[86]

(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.[87]

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. During CONOPS development, the commander must assimilate many variables under conditions of uncertainty to determine the essential military conditions, sequence of actions, and application of capabilities and associated forces to create effects and achieve objectives. Commanders and their staffs must be continually aware of the higher-level objectives and associated desired and undesired effects that influence planning at every juncture.[88]

(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.[89]

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

---

[86] JP 5-0, III-45 – 59.

[87] FM 3-12, 3-17 – 20.

[88] JP 5-0, III-64.

[89] FM 3-12, 3-20.

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.[90]

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.[91]

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.[92]

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.

---

[90] 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.

[91] JP 3-12, II-10 – 11.

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

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.[93]

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.[94]

---

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

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

## III. Cyberspace in Operations Orders (U.S. Army Doctrine)

1. **Operations Orders, fragmentary orders, and warning orders** include cyberspace operations information. The information is throughout the orders in different attachments found in Annex C and Annex H.

2. **Annexes to the operations order** also have cyberspace operations information. All annexes in paragraph 5, Command and Signal, have a subsection to describe the communications plan among the issuing force and interagency organizations including the primary and alternate means of communications. The subsection includes operations security requirements and indicates to refer to Annex H (Signal) as required. Tabs C, D, and E of Annex C contain operations information necessary for close coordination with cyberspace operations. The attachments to the base orders containing detailed information on cyberspace operations include:

a. Annex C – Operations.

(1) Appendix 12 – Cyberspace Electromagnetic Activities (Electronic Warfare Officer).

(2) Tab A – Offensive Cyberspace Operations.

(3) Tab B – Defensive Cyberspace Operations (RA & IDM).

(4) Tab C – Electronic Attack.

(5) Tab D – Electronic Protection.

(6) Tab E – Electronic Warfare Support.

b. Annex H – Signal.

(1) Appendix 1 – Defensive Cyberspace Operations.

(2) Appendix 2 – DODIN Operations.

(3) Appendix 3 – Voice, Video, and Data Network Diagrams.

(4) Appendix 4 – Satellite Communications.

(5) Appendix 5 – Foreign Data Exchanges.

(6) Appendix 6 – Spectrum Management Operations.

(7) Appendix 7 – Information Services.[95]

[95] FM 3-12, B-1

3. **Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) to Operations Plans And Orders**.

a. Commanders and staffs use Appendix 12 to Annex C to operations plans and orders to describe the Cyberspace and Electromagnetic Warfare (EW) operations support in a base plan or order.

b. This appendix describes Cyberspace Electromagnetic Activities (CEMA) and objectives. Complex cyberspace and EW support may require a schematic to show integration and synchronization requirements and task relationships. This includes a discussion of the overall cyberspace and EW concept of operations, required support, and specific details in element subparagraphs and attachments. This appendix contains the information needed to synchronize timing relationships of each of the elements related to cyberspace and EW operations. This appendix also includes related constraints, if appropriate.[96]

[96] FM 3-12, B-2

**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. The Chairman of the Joint Chiefs of Staff (CJCS), at the direction of the President or SecDef, issues an EXORD or other authorizing directive to initiate or conduct military operations.[97]

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).

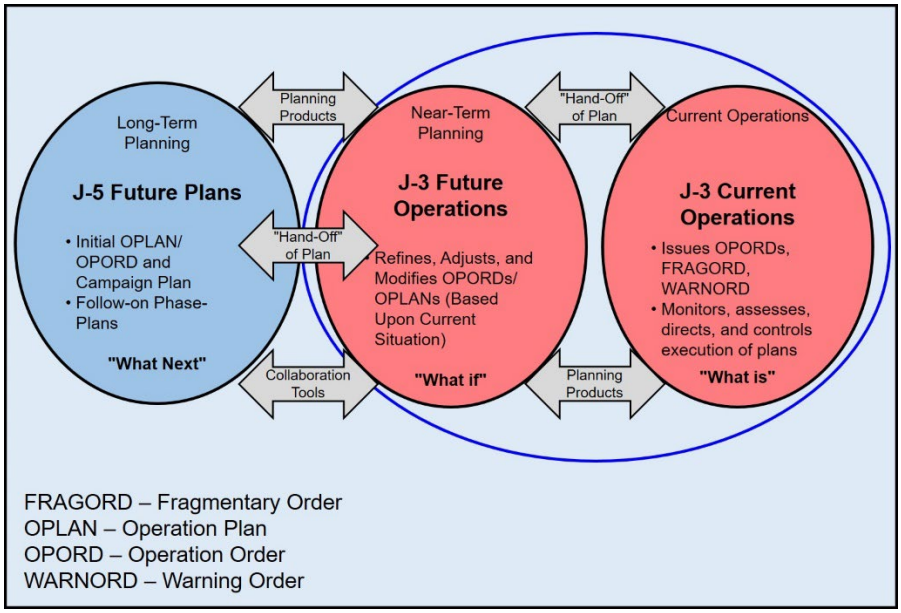


**Figure 4-1: Planning During Execution**[98]

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).

---

[97] JP 5-0, II-14.

[98] 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.

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.[99]

## 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.[100]

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

---

[99] 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.

[100] JP 3-12, IV-1 – 2.

(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).[101]

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<br><br>Title 28 | *Crimes and Criminal Procedure*<br><br>*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**[102]

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

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

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

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).[103]

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

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.[104]

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.[105]

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.[106]

---

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

[105] JP 3-12, IV-11 – 17.

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

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, U.S. Transportation Command, and U.S. Space Command.[107]

[107] 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.

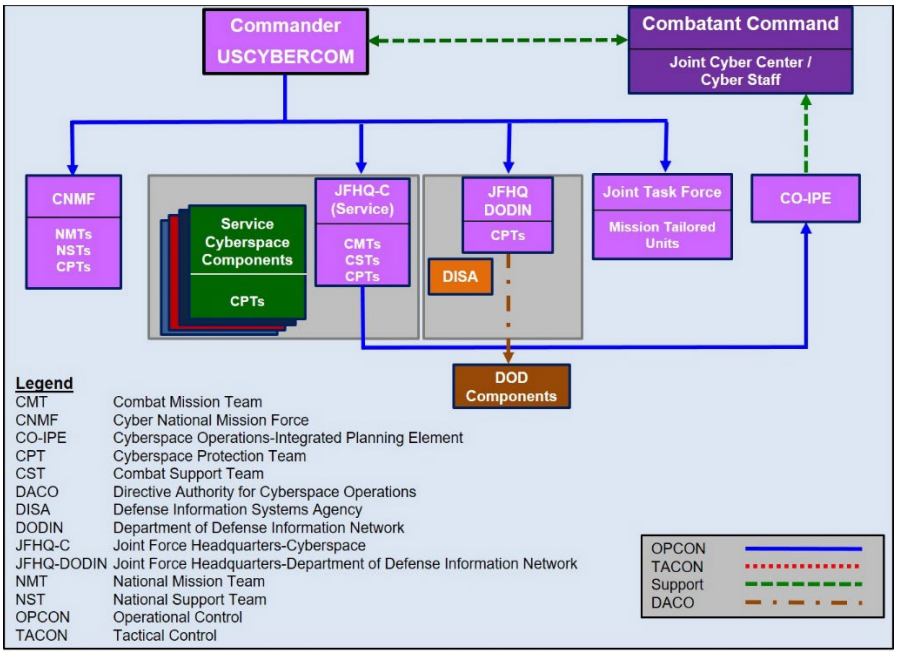


**Figure 4-3: Cyberspace Command and Control**
Adapted from JP 3-12, Figure IV-4.[108]

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

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

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.[109]

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,

[109] JP 3-12, IV-19 – 20.

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.[110]

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.[111]

## III. Cyber Effects Request Format (U.S. Army Doctrine)

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 and 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.[112]

a. Commanders use CO to create effects in and through cyberspace in support of military objectives.[113] Although it is possible for CO to produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate

---

[110] JP 3-12, IV-8 – 10.

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

[112] JP 5-0, IV-27 – 29.

[113] JP 3-12, x.

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.[114]

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.[115]

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.[116]

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.[117] The Cyber Effects Request Format (CERF) is the format forces use to request effects in and through cyberspace (see Figure 3-2). 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.[118]

a. The CERF includes the following supported operation information:

---

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

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

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

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

[118] FM 3-12, C-1 – 2.

(1) Supported OPLAN/CONPLAN/Order. Describe key details within the plan that the requested cyberspace attack will support.

(2) Supported Mission Statement. Describe the unit's essential task(s) and the purpose that the requested effect(s) will support.

(3) Supported Commander's Intent. Describe key information within the commander's intent that the requested effect(s) will support.

(4) Supported Commander's End State. Describe key information within the commander's end 200 state that the requested effect(s) will support.

(5) Supported Concept of Operations. Describe key information within the concept of operations that the requested effect(s) will support.

(6) Supported Objective (strategic, operational, and tactical). Describe the supported objective(s) that the requested effect(s) will directly support.

(7) Supported Tactical Objective/Task. Describe the tactical objectives and tasks that the requested effect(s) will directly or indirectly support.

b. The CERF also includes specific targeting and effects information:

(1) Type of Target.

- Indicate "scheduled" if specific dates, times, and or supporting conditions are known.
- Indicate "on-call" if trigger events or supporting conditions are known.

(2) Target Priority.

- Indicate "emergency" if the target requires immediate action. Indicate "priority" if the target requires a degree of urgency.
- Indicate "routine" if the target does not require immediate action or a degree of urgency beyond standard processing.

(3) Target Name. Enter the name of the target as codified in the Modernized Integrated Database.

(4) Target Location.

- Provide the target location
- Disregard if the request is for DCO-IDM.

(5) Target Description.

- Provide the target description.
- Describe the network node(s) wherein specific activities are to support DCO-IDM.

(6) Desired Effect.

- Enter deny, degrade, disrupt, destroy, or manipulate for OCO.
- Provide timing as "less than 96 hours", "96 hours to 90 days", or "greater than 90 days".

(7) Target Function. Enter target(s) primary function and additional functions if known.

(8) Target Significance. Describe why the target(s) is important to the enemy's or adversary's target system(s) or value in addition to its functions and expectations.

(9) Target Details. Describe additional information about the target(s) if known. This information should include any relevant device information such as type, number of users; activity; friendly actors in the area of operations; and surrounding/adjacent/parallel devices.

(10) Concept of Cyberspace Operations.

- Describe how the requested effect(s) would contribute to the commander's objectives and overall operations concept.
- Include the task, purpose, method, and end state.
- Describe the intelligence collection plan and specific assessment plan if known.
- Provide a reference to key directives and orders.

(11) Target Expectation Statement. According to CJCSI 3370.01, Enclosure D describes how the requested effect(s) will impact the target system(s). This description must address the following questions.

- How will the target system be affected if the target's function is neutralized, delayed, disrupted, or degraded? (Two examples are operational impact and psychological impact.)
- What is the estimated degree of impact on the target system(s)?
- What is the functional recuperation time estimated for the target system(s) if the target's function is neutralized, delayed, disrupted, or degraded?
- What distinct short-term or long-term military or political advantage/disadvantage do we expect if the target's function is neutralized, delayed, disrupted, or degraded?
- What is the expected enemy or adversary reaction to affecting the target's function?[119]

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

**Intentionally Blank**

# Chapter 5: Operations in the Homeland

*"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors."*

—President Joseph R. Biden, Jr.[120]

## 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.[121]

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.[122]

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.

---

[120] Joseph R. Biden, Jr., President of the USA, *Executive Order on Improving the Nation's Cybersecurity*, (Washington, DC: The Whitehouse, 12 May 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

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

[122] 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.

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).[123]

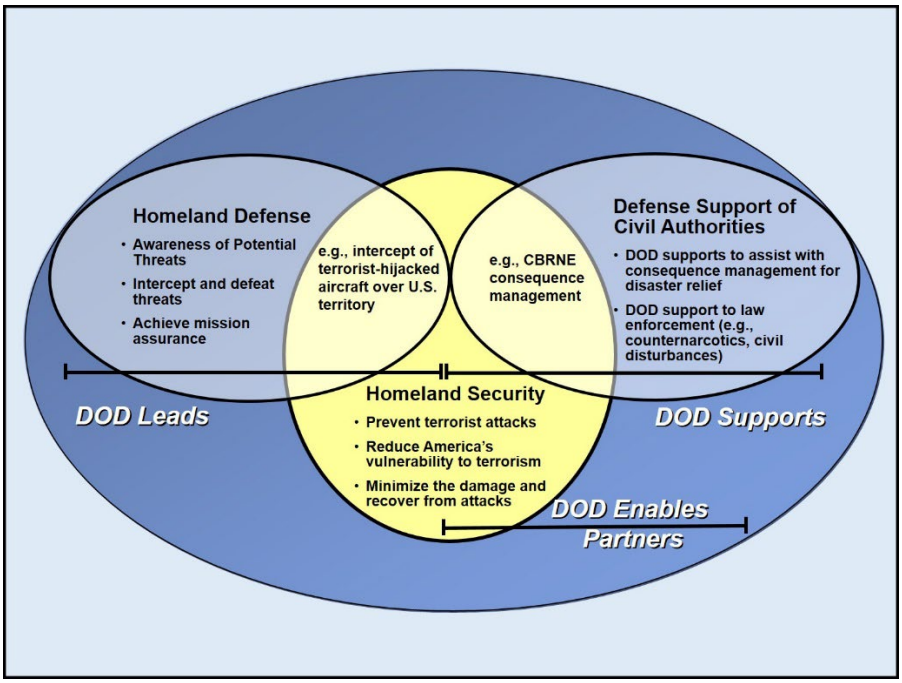


**Figure 5-1: Active, Layered Defense of the United States**

## 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.

[123] JP 3-27, I-1 – 3.

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.[124]

## 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 17 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 summarized below.

---

[124] Critical Infrastructure Sectors, linked from the *Department of Homeland Security Home Page*, https://www.dhs.gov/critical-infrastructure-sectors.

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.[125]

## 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 objectives. One of these goals is **defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident**. A "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).

a. 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) and Defense Industrial Base (DIB) entities. DOD will defend forward to halt or degrade cyberspace operations targeting the Department, and will collaborate to strengthen the cybersecurity and resilience of DOD, DCI, and DIB networks and systems.

---

[125] DOD Protected Critical Infrastructure Program, linked from *Under Secretary of Defense for Policy Home Page*, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Global-Security/Defense-Critical-Infrastructure-Program/Roles/.

b. 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. DOD's 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 (see Figure 5-2).[126]

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.[127]

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.[128]

---

[126] *James N. Mattis, Summary Department of Defense Cyber Strategy 2018*, 2 – 3.

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

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

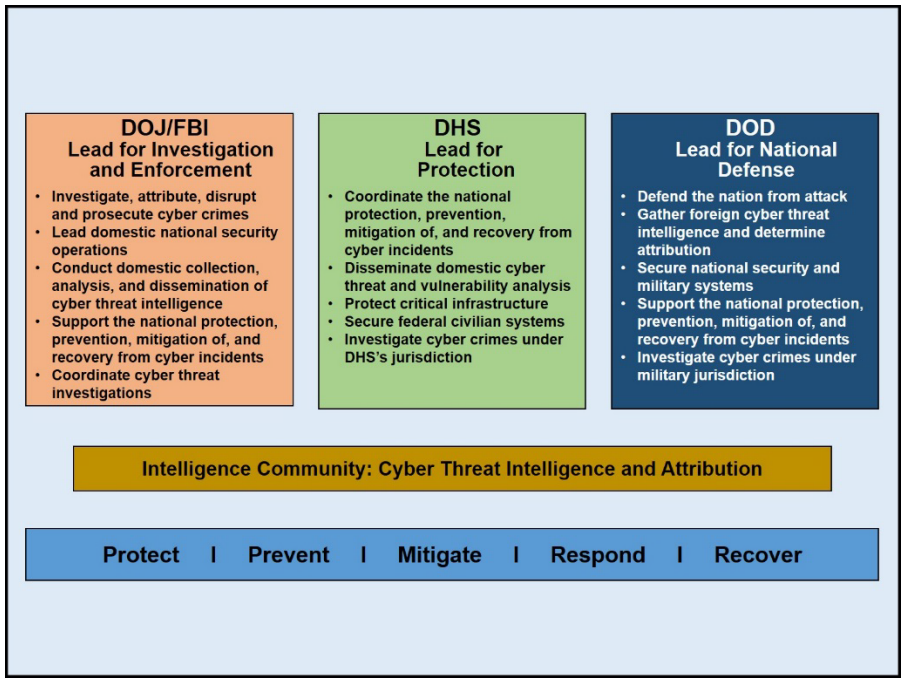


**Figure 5-2: National Cybersecurity Roles and Responsibilities**

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.[129]

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.[130]

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

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

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

threshold of the use of force and outside of the context of armed conflict, but cumulatively accrue strategic gains to our adversaries.[131] 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.[132]

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.[133]

---

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

[132] 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.

[133] JP 3-12, I-13 – 14.

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.[134]

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.[135] 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

---

[134] *DOD Cyber Strategy*, 23.

[135] *DOD Cyber Strategy*, 2.

infrastructure issues. Likewise, DOD coordinates and integrates when necessary with DHS for support of efforts to protect the DIB.[136]

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.[137]

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.[138]

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.[139] 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.[140]

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

---

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

[137] JP 3-12, I-12 – 13.

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

[139] *DOD Cyber Strategy*, 22.

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

well as provide support to LE, HD, and DSCA activities in support of national objectives.[141]

(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.[142]

(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 personnel, DOD civilian personnel, and DOD 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).[143]

## 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.

---

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

[142] 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.

[143] 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, Incorporating Change 4, 21 May 2021), 2 – 3.

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.[144]

## 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.[145]

[144] JP 3-12, III-10 – 11.

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

**Intentionally Blank**

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

**Appendix A includes:**

I. **U.S. Strategy and Policy**
   - **Cyberspace Solarium Commission Report**
   - **Interim National Security Strategic Guidance**
   - **Presidential Executive Order on Improving the Nation's Cybersecurity**
   - **National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems**

II. **Department of State Cyberspace Policy**
   - **Joint Statement on Advancing Responsible State Behavior in Cyberspace**
   - **Protecting American Cyber Interests through International Engagement**
   - **Deterring Adversaries and Better Protecting the American People from Cyber Threats**

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

IV. **Department of Justice Cyber Strategy and Guidance**
   - **DOJ 2022 Comprehensive Cyber Review**
   - **FBI Cyber Strategy**

V. **Department of Defense Strategy**
   - **DOD Cyber Strategy**
   - **Commander, USCYBERCOM Congressional Testimony**

VI. **U.S. Cyber Law Guidance**
   - **DOS Remarks on International Law and Stability in Cyberspace**
   - **DOD Domestic and International Cyber Law Considerations**
   - **DOD Law of War Manual**

# I. U.S. Strategy and Policy

## A. Cyberspace Solarium Commission Report

The 2019 National Defense Authorization Act chartered the U.S. Cyberspace Solarium Commission. The President and Congress tasked the Commission to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy? The Commission released its report in March 2020 (the official report can be found at: https://www.solarium.gov/report).

**Our Strategy**.

After conducting an extensive study including over 300 interviews, a competitive strategy event modeled after the original Project Solarium in the Eisenhower administration, and stress tests by external red teams, the Commission advocates a new strategic approach to cybersecurity: layered cyber deterrence. The desired end state of layered cyber deterrence is a reduced probability and impact of cyberattacks of significant consequence. The strategy outlines three ways to achieve this end state:

1. ***Shape behavior***. The United States must work with allies and partners to promote responsible behavior in cyberspace.

2. ***Deny benefits***. The United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to American disadvantage, and at little cost to themselves. This new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.

3. ***Impose costs***. The United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace.

Each of the three ways described above involves a deterrent layer that increases American public- and private-sector security by altering how adversaries perceive the costs and benefits of using cyberspace to attack American interests.

While deterrence is an enduring American strategy, there are two factors that make layered cyber deterrence bold and distinct. First, the approach prioritizes deterrence by denial, specifically by increasing the defense and security of cyberspace through resilience and public- and private-sector collaboration. Reducing the vulnerabilities adversaries can target denies them opportunities to attack American interests through cyberspace. Second, the strategy incorporates the concept of "defend forward" to reduce the frequency and severity of attacks in cyberspace that do not rise to a level that would warrant the full spectrum of retaliatory responses, including military responses. The Commission integrates defend forward into a national strategy for securing cyberspace using all the instruments of power. Defend forward posits that to disrupt and defeat ongoing adversary campaigns, the United States must proactively observe, pursue, and counter adversaries' operations and impose costs short of armed conflict. This posture signals to adversaries that the U.S. government will respond to cyberattacks, even those below the level of armed conflict that do not cause physical destruction or death, with all the tools at its disposal and consistent with international law.

The Cyberspace Solarium Commission report consists of over 80 recommendations which are organized into 6 pillars. These 6 pillars are as follows:

1. ***Reform the U.S. Government's Structure and Organization for Cyberspace***. While cyberspace has transformed the American economy and society, the government has not kept up. Existing government structures and jurisdictional boundaries fracture cyber policymaking

processes, limit opportunities for government action, and impede cyber operations. Rapid, comprehensive improvements at all levels of government are necessary to change these dynamics and ensure that the U.S. government can protect the American people, their way of life, and America's status as a global leader.

2. ***Strengthen Norms and Non-Military Tools***. A system of norms, built through international engagement and cooperation, promotes responsible behavior and dissuades adversaries from using cyber operations to undermine American interests. The United States and others have agreed to norms of responsible behavior for cyberspace, but they go largely unenforced. The United States can strengthen the current system of cyber norms by using non-military tools, including law enforcement actions, sanctions, diplomacy, and information sharing, to more effectively persuade states to conform to these norms and punish those who defect from them. A coalition of like-minded allies and partners willing to collectively support a rules-based international order in cyberspace will better hold malign actors accountable.

3. ***Promote National Resilience***. Resilience, the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior, is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends. National resilience efforts rely on the ability of both the United States public and private sectors to accurately identify, assess, and mitigate risk across all elements of critical infrastructure. The nation must be sufficiently prepared to respond to and recover from an attack, sustain critical functions even under degraded conditions, and, in some cases, restart critical functionality after disruption.

4. ***Reshape the Cyber Ecosystem***. Raising the baseline level of security across the cyber ecosystem – the people, processes, data, and technology that constitute and depend on cyberspace – will constrain and limit adversaries' activities. Over time, this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes. In some cases, that requires aligning market forces. In other cases, where those forces either are not present or do not adequately address risk, the U.S. government must explore legislation, regulation, executive action, and public-as well as private-sector investments.

5. ***Operationalize Cybersecurity Collaboration with the Private Sector***. Unlike in other physical domains, in cyberspace the government is often not the primary actor. It must support and enable the private sector. The government must build and communicate a better understanding of threats, with the specific aim of informing private-sector security operations, directing government operational efforts to counter malicious cyber activities, and ensuring better common situational awareness for collaborative action with the private sector. While recognizing that private-sector entities have primary responsibility for the defense and security of their networks, the U.S. government must bring to bear its unique authorities, resources, and intelligence capabilities to support these actors in their defensive efforts.

6. ***Preserve and Employ the Military Instrument of National Power***. Future crises and conflicts will almost certainly contain a cyber component. In this environment, the United States must defend forward to limit malign adversary behavior below the level of armed attack, deter conflict, and, if necessary, prevail employing the full spectrum of its capabilities. Conventional weapons and nuclear capabilities require cybersecurity and resilience to ensure that the United States preserves credible deterrence and the full range of military response options. Across the spectrum from competition to crisis and conflict, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives through cyberspace.

Source: https://www.solarium.gov/report.

## B. Interim National Security Strategic Guidance

President Biden released the Interim National Security Strategic Guidance in March 2021. An excerpt of the guidance document is provided below, the full document can be found at: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

### Introduction

**Today, more than ever, America's fate is inextricably linked to events beyond our shores. We confront a global pandemic, a crushing economic downturn, a crisis of racial justice, and a deepening climate emergency. We face a world of rising nationalism, receding democracy, growing rivalry with China, Russia, and other authoritarian states, and a technological revolution that is reshaping every aspect of our lives. Ours is a time of unprecedented challenges, but also unmatched opportunity.**

This moment calls upon us to lean forward, not shrink back – to boldly engage the world to keep Americans safe, prosperous, and free. It requires a new and broader understanding of national security, one that recognizes that our role in the world depends upon our strength and vitality here at home. It demands creative approaches that draw on all the sources of our national power: our diversity, vibrant economy, dynamic civil society and innovative technological base, enduring democratic values, broad and deep network of partnerships and alliances, and the world's most powerful military. Our task is to ensure these advantages endure, by building back better at home and reinvigorating our leadership abroad. From a position of renewed strength, America can meet any challenge.

Together, we will demonstrate not only that democracies can still deliver for our people, but that democracy is essential to meeting the challenges of our time. We will strengthen and stand behind our allies, work with like-minded partners, and pool our collective strength to advance shared interests and deter common threats. We will lead with diplomacy. We will renew our commitment to global development and international cooperation, while also making smart, disciplined investments in our national defense. We will address the crises of today while promoting resilience, innovation, competitiveness, and truly shared prosperity for the future. We will recommit to realizing our ideals. We will modernize our national security institutions and processes, while ensuring we take advantage of the full diversity of talents required to address today's complex challenges. And in everything we do, we will aim to make life better, safer, and easier for working families in America.

### The Global Security Landscape

We cannot pretend the world can simply be restored to the way it was 75, 30, or even four years ago. We cannot just return to the way things were before. In foreign policy and national security, just as in domestic policy, we have to chart a new course.

- Recent events show all too clearly that many of the biggest threats we face respect no borders or walls, and must be met with collective action.
- At a time when the need for American engagement and international cooperation is greater than ever, however, democracies across the globe, including our own, are increasingly under siege.
- We must also contend with the reality that the distribution of power across the world is changing, creating new threats.
- This work is urgent, because the alliances, institutions, agreements, and norms underwriting the international order the United States helped to establish are being tested.

- Finally, running beneath many of these broad trends is a revolution in technology that poses both peril and promise.

**Our National Security Priorities**

The vital national interests of the United States have endured since the founding of the Republic. Today, advancing these interests requires a new approach updated for the challenges of our time.

- It is our most solemn obligation to protect the security of the American people.
- We have an enduring interest in expanding economic prosperity and opportunity.
- We must remain committed to realizing and defending the democratic values at the heart of the American way of life.

**Cybersecurity**

As we bolster our scientific and technological base, **we will make cybersecurity a top priority**, strengthening our capability, readiness, and resilience in cyberspace. We will elevate cybersecurity as an imperative across the government. We will work together to manage and share risk, and we will encourage collaboration between the private sector and the government at all levels in order to build a safe and secure online environment for all Americans. We will expand our investments in the infrastructure and people we need to effectively defend the nation against malicious cyber activity, providing opportunities to Americans of diverse backgrounds as we build an unmatched talent base. We will renew our commitment to international engagement on cyber issues, working alongside our allies and partners to uphold existing and shape new global norms in cyberspace. And we will hold actors accountable for destructive, disruptive, or otherwise destabilizing malicious cyber activity, and respond swiftly and proportionately to cyberattacks by imposing substantial costs through cyber and noncyber means.

Source: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

## C. Presidential Executive Order on Improving the Nation's Cybersecurity

On 12 May 2021, President Biden signed an Executive Order aimed at strengthening cybersecurity. The following is the Fact Sheet that provides an overview of the order (the Executive Order can be found at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/):

**FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks**

Today, President Biden signed an Executive Order to improve the nation's cybersecurity and protect federal government networks. Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities, including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents.

This Executive Order makes a significant contribution toward modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. It is the first of many ambitious steps the Administration is taking to modernize national cyber defenses. However, the Colonial Pipeline incident is a reminder that federal action alone is not enough. Much of our domestic critical infrastructure is owned and operated by the private sector, and those private sector companies make their own determination regarding cybersecurity investments. We encourage private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.

Specifically, the Executive Order the President is signing today will:

> **Remove Barriers to Threat Information Sharing Between Government and the Private Sector.** The Executive Order ensures that IT Service Providers are able to share information with the government and requires them to share certain breach information. IT providers are often hesitant or unable to voluntarily share information about a compromise. Sometimes this can be due to contractual obligations; in other cases, providers simply may be hesitant to share information about their own security breaches. Removing any contractual barriers and requiring providers to share breach information that could impact Government networks is necessary to enable more effective defenses of Federal departments, and to improve the Nation's cybersecurity as a whole.
>
> **Modernize and Implement Stronger Cybersecurity Standards in the Federal Government.** The Executive Order helps move the Federal government to secure cloud services and a zero-trust architecture, and mandates deployment of multifactor authentication and encryption with a specific time period. Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors. The Federal government must lead the way and increase its adoption of security best practices, including by employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multifactor authentication and encryption.
>
> **Improve Software Supply Chain Security.** The Executive Order will improve the security of software by establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater

visibility into their software and making security data publicly available. It stands up a concurrent public-private process to develop new and innovative approaches to secure software development and uses the power of Federal procurement to incentivize the market. Finally, it creates a pilot program to create an "energy star" type of label so the government – and the public at large – can quickly determine whether software was developed securely. Too much of our software, including critical software, is shipped with significant vulnerabilities that our adversaries exploit. This is a long-standing, well-known problem, but for too long we have kicked the can down the road. We need to use the purchasing power of the Federal Government to drive the market to build security into all software from the ground up.

**Establish a Cybersecurity Safety Review Board.** The Executive Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. Too often organizations repeat the mistakes of the past and do not learn lessons from significant cyber incidents. When something goes wrong, the Administration and private sector need to ask the hard questions and make the necessary improvements. This board is modeled after the National Transportation Safety Board, which is used after airplane crashes and other incidents.

**Create a Standard Playbook for Responding to Cyber Incidents.** The Executive Order creates a standardized playbook and set of definitions for cyber incident response by federal departments and agencies. Organizations cannot wait until they are compromised to figure out how to respond to an attack. Recent incidents have shown that within the government the maturity level of response plans vary widely. The playbook will ensure all Federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts.

**Improve Detection of Cybersecurity Incidents on Federal Government Networks.** The Executive Order improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government. Slow and inconsistent deployment of foundational cybersecurity tools and practices leaves an organization exposed to adversaries. The Federal government should lead in cybersecurity, and strong, Government-wide Endpoint Detection and Response (EDR) deployment coupled with robust intra-governmental information sharing are essential.

**Improve Investigative and Remediation Capabilities.** The Executive Order creates cybersecurity event log requirements for federal departments and agencies. Poor logging hampers an organization's ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact. Robust and consistent logging practices will solve much of this problem.

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

## D. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure

On 28 July 2021, President Biden signed the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*.

Protection of our Nation's critical infrastructure is a responsibility of the government at the Federal, State, local, Tribal, and territorial levels and of the owners and operators of that infrastructure. The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issues confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States.

Section 1. Policy. It is the policy of my Administration to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions, defined as the functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof.

Sec. 2. Industrial Control Systems Cybersecurity Initiative. Accordingly, I have established an Industrial Control Systems Cybersecurity Initiative (Initiative), a voluntary, collaborative effort between the Federal Government and the critical infrastructure community to significantly improve the cybersecurity of these critical systems. The primary objective of this Initiative is to defend the United States' critical infrastructure by encouraging and facilitating deployment of technologies and systems that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks. The goal of the Initiative is to greatly expand deployment of these technologies across priority critical infrastructure.

Sec. 3. Furthering the Industrial Control Systems Cybersecurity Initiative. The Initiative creates a path for Government and industry to collaborate to take immediate action, within their respective spheres of control, to address these serious threats. The Initiative builds on, expands, and accelerates ongoing cybersecurity efforts in critical infrastructure sectors and is an important step in addressing these threats. We cannot address threats we cannot see; therefore, deploying systems and technologies that can monitor control systems to detect malicious activity and facilitate response actions to cyber threats is central to ensuring the safe operations of these critical systems. The Federal Government will work with industry to share threat information for priority control system critical infrastructure throughout the country.

> (a) The Initiative began with a pilot effort with the Electricity Subsector, and is now followed by a similar effort for natural gas pipelines. Efforts for the Water and Wastewater Sector Systems and Chemical Sector will follow later this year.
>
> (b) Sector Risk Management Agencies, as defined in section 9002(a)(7) of Public Law 116-283, and other executive departments and agencies (agencies), as appropriate and consistent with applicable law, shall work with critical infrastructure stakeholders and owners and operators to implement the principles and policy outlined in this memorandum.

Sec. 4. Critical Infrastructure Cybersecurity Performance Goals. Cybersecurity needs vary among critical infrastructure sectors, as do cybersecurity practices. However, there is a need for baseline cybersecurity goals that are consistent across all critical infrastructure sectors, as well

as a need for security controls for select critical infrastructure that is dependent on control systems.

(a) Pursuant to section 7(d) of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), the Secretary of Homeland Security, in coordination with the Secretary of Commerce (through the Director of the National Institute of Standards and Technology) and other agencies, as appropriate, shall develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.

(b) This effort shall begin with the Secretary of Homeland Security issuing preliminary goals for control systems across critical infrastructure sectors no later than September 22, 2021, followed by the issuance of final cross-sector control system goals within 1 year of the date of this memorandum. Additionally, following consultations with relevant agencies, the Secretary of Homeland Security shall issue sector-specific critical infrastructure cybersecurity performance goals within 1 year of the date of this memorandum. These performance goals should serve as clear guidance to owners and operators about cybersecurity practices and postures that the American people can trust and should expect for such essential services. That effort may also include an examination of whether additional legal authorities would be beneficial to enhancing the cybersecurity of critical infrastructure, which is vital to the American people and the security of our Nation.

Sec. 5. General Provisions.

a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations, where funding assistance may be required to implement control system cybersecurity recommendations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

## II. Department of State Cyberspace Policy

## A. Joint Statement on Advancing Responsible State Behavior in Cyberspace

The Department of State released the following joint statement on 23 September 2019.

The following text is a joint statement affirmed by these countries: Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom, and the United States.

Joint Statement on Advancing Responsible State Behavior in Cyberspace

Information technology is transforming modern life, driving innovation and productivity, facilitating the sharing of ideas, of cultures, and promoting free expression. Its benefits have brought the global community closer together than ever before in history. Even as we recognize the myriad benefits that cyberspace has brought to our citizens and strive to ensure that humanity can continue to reap its benefits, a challenge to this vision has emerged. State and non-state actors are using cyberspace increasingly as a platform for irresponsible behavior from which to target critical infrastructure and our citizens, undermine democracies and international institutions and organizations, and undercut fair competition in our global economy by stealing ideas when they cannot create them.

Over the past decade, the international community has made clear that the international rules-based order should guide state behavior in cyberspace. UN member states have increasingly coalesced around an evolving framework of responsible state behavior in cyberspace (framework), which supports the international rules-based order, affirms the applicability of international law to state-on-state behavior, adherence to voluntary norms of responsible state behavior in peacetime, and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber incidents. All members of the United Nations General Assembly have repeatedly affirmed this framework, articulated in three successive UN Groups of Governmental Experts reports in 2010, 2013, and 2015.

We underscore our commitment to uphold the international rules-based order and encourage its adherence, implementation, and further development, including at the ongoing UN negotiations of the Open Ended Working Group and Group of Governmental Experts. We support targeted cybersecurity capacity building to ensure that all responsible states can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyber activity. We reiterate that human rights apply and must be respected and protected by states online, as well as offline, including when addressing cybersecurity.

As responsible states that uphold the international rules-based order, we recognize our role in safeguarding the benefits of a free, open, and secure cyberspace for future generations. When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace.

We call on all states to support the evolving framework and to join with us to ensure greater accountability and stability in cyberspace.

Source: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

## B. Protecting American Cyber Interests through International Engagement

In collaboration with colleagues across the federal government, the Department of State produced *Recommendations to the President on Protecting American Cyber Interests through International Engagement*. The following is an excerpt of the document:

### 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: https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf.

## C. Deterring Adversaries and Better Protecting the American People from Cyber Threats

In collaboration with colleagues across the federal government, the Department of State produced *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. The following is an excerpt of the document:

### Assessment of Deterring Malicious Cyber Activities as a Policy Challenge

Strategies for deterring malicious cyber activities require a fundamental rethinking. Cyber capabilities can be used to carry out malicious acts in peacetime, periods of increasing international tensions, crisis situations as well as during armed conflicts. Both state actors and numerous non-state actors possess such capabilities.

Although the United States has achieved important successes in recent years in promoting a framework for responsible state behavior in cyberspace, the continued prevalence of state-sponsored cyber incidents that rise to the level of a national security concern has demonstrated that the framework is necessary but not sufficient to protect against cyber threats. To achieve the stability necessary to maintain and promote the U.S. vision for an "open, interoperable, reliable, and secure internet," the United States and its likeminded partners must be able to deter destabilizing state conduct in cyberspace.

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. This report proposes developing a broader menu of consequences that the United States can swiftly impose following a significant cyber incident, and taking steps to help resolve attribution and policy challenges that limit U.S. flexibility to act.

In addition, the U.S. government must seek to deter malicious non-state actors. The U.S. government can impose significant consequences on such actors, but their strength as a deterrent partially depends on the actors' certainty that they will become subject to those consequences. Challenges related to attribution, obtaining evidence located abroad, and seeking extradition, expulsion, or foreign prosecution, impact U.S. efforts to deter malicious non-state cyber actors.

### 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.

As the United States further strengthens its ability to respond to states' malicious cyber activities, it should develop tailored strategies for deterring each of its key adversaries in cyberspace.

Non-state actors are susceptible to both deterrence by cost-imposition and deterrence by denial. However, because certain actors, including terrorists, may not be as sensitive to the threat of cost imposition, the United States must also focus on increasing the operational cost and complexity for non-state actors to achieve their goals, including through efforts to prevent and disrupt access to malicious cyber capabilities.

Source: https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

# III. 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: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Fact-Sheet.pdf.

## B. Framework for Improving Critical Infrastructure Cybersecurity

The National Institute of Standards and Technology released this framework (version 1.1) on 16 April 2018. The following is an excerpt of the Executive Summary, The full document can be found at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

### Executive Summary

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 risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

To better address these risks, the Cybersecurity Enhancement Act of 2014[1] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636, and continues to evolve according to CEA, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business and organizational 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 Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission 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, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. 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 security and resilience.

---

[1]See 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.govinfo.gov/content/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf.

The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

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. They also will vary in how they customize practices described in the Framework. 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.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs. There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

# IV. Department of Justice Cyber Strategy and Guidance

## A. DOJ Comprehensive Cyber Review

The following is an excerpt from the July 2022 Comprehensive Cyber Review https://www.justice.gov/dag/page/file/1520341/download:

**Executive Summary**

In May 2021, Deputy Attorney General Lisa O. Monaco directed the Department of Justice to conduct a comprehensive review of the Department's cyber-related activities and to develop actionable recommendations to enhance and expand the Department's efforts. This report summarizes the findings from that review. It evaluates many different facets of the Department's cyber capabilities, both "offensive" (i.e., how it investigates, prosecutes, and combats cyber threats) and "defensive" (i.e., how it protects its own networks from continuous malicious cyber activity). It also evaluates the Department's engagement with various governmental and private-sector partners; its preparation for emerging technologies; and the ways in which it is building and retaining its cyber workforce for the future.

As stated in the memorandum announcing the review, the focus has been on actionable recommendations to enhance and expand the Department's efforts against fast-changing cyber threats. To that end, the review has already made a number of interim recommendations that Department leadership has accepted and implemented. These include:

- The creation of the National Cryptocurrency Enforcement Team (NCET) within the Department's Criminal Division, which focuses on combating illicit uses of cryptocurrency.
- The launch of the Civil Cyber-Fraud Initiative (CCFI) by the Department's Civil Division. The CCFI uses the Department's authorities under the False Claims Act to pursue civil actions against government grantees and contractors—including those under contract with the Department of Justice—who fail to meet cybersecurity obligations.
- The development of a new Cyber Fellowship within the Department, designed to foster a new generation of prosecutors and attorneys equipped to handle emerging cybercrime and cyber-based national security threats.
- The rollout of additional cybersecurity measures designed to improve the Department's email security. These measures included mandatory Departmentwide encryption training for Department personnel and additional technical measures to protect against phishing and related techniques.

**Disruption, Accountability, and Deterrence**. The threats in cyberspace evolve with unmatched speed. For the Department to disrupt these attacks and hold accountable those responsible, it will need to move with almost unprecedented agility. This past year has shown the Department moving to keep pace with evolving cyber threats. For example, even before the series of significant ransomware attacks during 2021, the Department began to accelerate its focus on the threat through the creation of the Ransomware and Digital Extortion Task Force. Today, the Department is investigating over 100 different ransomware variants and ransomware groups that have caused billions of dollars in damage. The Department also had some notable successes in the last year, including the recovery of approximately $2.3 million in ransom paid to the Colonial Pipeline attackers; the recovery of ransom keys that the Department used to assist victims of the Kaseya ransomware attack; and the arrests of multiple individuals suspected of being involved in these and other significant attacks.

The Department has also quickly adapted to the continued threat of cryptocurrency's illicit uses. While the Department for years has traced cryptocurrency in investigations and combated money laundering involving cryptocurrency, in the last year it has taken additional steps to strengthen its institutional expertise on digital currency. The newly created NCET is now staffed with a Director and more than a dozen prosecutors with backgrounds in money laundering, computer crimes, regulatory policy, forfeiture, and other relevant areas. Additionally, the FBI has created the Virtual Asset Unit (VAU), a new partnership between the FBI's Criminal Investigative and Cyber Divisions that will merge their respective expertise in cryptocurrency.

The Department continues to play a unique and critical role in addressing almost every cyber threat. And as many recent examples show, the Department can be impactful against these threats even before prosecution and arrest. Last year saw the Department successfully deploy a number of novel means of disrupting threats, including the seizure of ransomware payments (including the aforementioned Colonial Pipeline seizure) and the court-authorized removal of malware from hundreds of infected computers. These successes should serve as "proof of concept" and renew the Department's commitment to using its full suite of tools to disrupt cyber threats. One point of emphasis to come out of this review, however, is that the Department can significantly amplify its own efforts by working more closely with its partners and allies – those elsewhere in the U.S. Government; those in like-minded nations; those in state, local, tribal, and territorial governments; and those in the private sector. Given the transnational nature of significant cyber threats – and the fact that many are state-sponsored or state-sanctioned – the Department needs to couple its own tools with those of its partners.

For this reason, the Department will designate an experienced Department prosecutor to serve as the first-ever Cyber Operations International Liaison (COIL), whose responsibility will be to work with applicable Department components and European allies to increase the tempo of or otherwise enable operations and other disruptive actions against top-tier cyber actors, including charges, arrests, extraditions, asset seizures, and the dismantlement of infrastructure.

The Department has a proven track record of working with these partners, but it can further improve its coordination, including through some recommendations proposed in this report. One recommendation is to require all prosecutors handling significant cyber investigations with transnational links to consult with attorneys in the Department's Criminal Division (CRM) and National Security Division (NSD) who have experience and training in working with the relevant partners to ensure a multi-front response to an ongoing threat. Another recommendation is to continue to assign Department personnel to other Departments that have different authorities and tools; based on a recommendation during this review, for example, a Department attorney for the first time was seconded to the Defense Department's Cyber Command in an effort to increase interagency partnerships. The collective goal of these recommendations is to ensure that the Department's thinking about whole-of-government and international campaigns is more proactive and begins as early as possible in an investigation.

**Strengthening the Department's Defenses and Building Resilience**. While the Department plays a key role in defending others from malicious cyber activity, it must also ensure that its networks and systems are properly defended from a continuous barrage of state-sponsored and criminal attacks. Since the December 2020 breach linked to the global SolarWinds supply-chain compromise and related breaches of Microsoft Office 365 (O365) systems, the Department has redoubled its efforts to remediate against that intrusion and protect against another significant compromise.

The Department's own internal review of its preparedness coincided with the issuance of "Executive Order on Improving the Nation's Cybersecurity" (E.O. 14028), which sets forth new measures that all federal departments and agencies must take to improve the U.S.

Government's collective cybersecurity. This review's assessment of the Department's "cyberdefenses" focused on how the Department could better follow the directives set forth in E.O. 14028, including specific multi-factor authentication, data-at-rest encryption, logging, and cloud computing standards. However, a number of additional areas were flagged as areas where the Department could improve its practices in order to increase its cybersecurity. These included the Department's electronic communications practices (including email and document-transfer practices), mobile device security, and contractor cybersecurity requirements. For each area identified, this report recommends steps to avoid unnecessary exposure to another significant cyber incident.

The review also concluded that the Department would benefit from updated response plans to a significant cyber intrusion into its own systems. The review found, for example, that the existing policies for the information security team had not been updated to include the lessons learned from the December 2020 breach. The review also concluded that planning should not just be limited to information security personnel and privacy officers, but rather involve the leadership of all offices and divisions within the Department. To that end, the review recommended that separate cyber-incident response materials (called the Justice Cyber Incident Playbook) be prepared for the Department's leadership, so that the response to cyber incidents will involve those who understand the operational significance of a breach and can direct relevant personnel to take remedial actions.

**Ensuring Policies and Workforce Reflect the Department's Priorities and Values**. This review considered two other important sets of issues that will be critical as the Department positions itself for the future: how it will deal with emerging technologies, and what can be done to ensure the Department has a qualified and supported workforce.

Many offices and divisions within the Department already spend significant time and effort identifying the impact of new technologies, considering their impact on civil liberties, public safety, competition, or the Department's own investigative capabilities. Too often, however, these efforts to evaluate technologies are siloed, such that the cross-cutting expertise across the Department has not been leveraged. To that end, the report focuses on developing ways to take an interdisciplinary approach to evaluating new technologies.

The review recommends that this work start with an Emerging Technology Board, whose responsibility will be to ensure that the Department evaluates the implications of new technology by enlisting the diverse expertise across the Department. This Board will help coordinate disparate efforts to avoid duplication, as well as ensure that all stakeholders within the Department have a chance to consider these important issues.

When it comes to its own use of these technologies, the Department also needs to ensure that it has appropriate frameworks in place to avoid misuse of new technologies. Based on a recommendation from this review, for example, the Department recently completed the Principles for the Ethical Use of Artificial Intelligence, which will serve as a way for the Department to ensure that artificial intelligence is deployed appropriately, whether assisting in personnel decisions or identifying suspects in an investigation. The report identifies other areas for similar focus in the future.

Finally, the report considers ways in which the Department can build its cyber workforce for the future. Whether a systems engineer, cyber prosecutor, cyber policy expert, special agent, or analyst, Department employees are talented and will continue to receive job offers from other agencies and the private sector. The risk of personnel attrition is heightened by the fact that other departments within the U.S. Government have recently begun to offer more competitive salaries to cyber experts. In many cases, hiring offices within the Department do not appear to be aware of similar authorities. As a first step, therefore, the review recommends that hiring

offices receive information and instruction on available and under-utilized incentives for some of the most competitive positions.

**Note**. This report builds on the Department's prior work to address cyber challenges, including the *2018 Report of the Attorney General's Cyber Digital Task Force* and the *2020 Cryptocurrency Enforcement Framework*, and therefore does not repeat many of the overviews of the Department's work or legislative recommendations that have not yet been enacted by Congress. A central goal of the Comprehensive Cyber Review is to identify concrete and actionable ways the Department can draw on the full range of its criminal, civil, national security, and administrative authorities and resources to confront the multidimensional cyber challenge. Many of the recommendations contained in this report reflect practices and efforts already underway within the Department, led by career attorneys, agents, analysts, and others, and reflect lessons learned in numerous individual cases.

Source: https://www.justice.gov/dag/page/file/1520341/download.

## B. FBI Cyber Strategy

The following is an excerpt from the FBI's Cyber Strategy:

**Vision**

For over a century, the FBI has been investigating crimes and collecting intelligence to protect the American public. As threats have evolved, so has our strategy. The FBI's new cyber strategy not only focuses on how we will confront the unique challenges faced in cyberspace, but also why we pursue our cyber mission: so ***the American people have safety, security, and confidence in a digitally connected world***.

Safety is knowing that criminal and nation state actors are being held to account for targeting and compromising U.S. citizens, companies, and organizations. Accountability may come in a variety of forms ranging from indictments and red notices to sanctions, diplomatic pressure, or cyber operations.

Security is receiving actionable alerts about system and network vulnerabilities, derived from intelligence that only the FBI and its partners can provide. It means notifying targeted entities before they experience a breach and providing them with the tools and information necessary to defend themselves. We are committed to sharing as much as possible as quickly as possible so the public is alerted and prepared.

Confidence is knowing that the federal government is combatting these threats with fierce urgency and that if you become a victim, you will receive the attention you deserve. The FBI is working 24/7 and in tandem with the rest of the federal government and industry to break down walls and attack the cyber threat as a united front. Our strategy drives us, but our vision inspires us. Together we'll fight to make it our reality.

**Mission**

Our Focus – what we do every day. To impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building on a century of innovation

Our Promise – compassion as we seek justice. In pursuing our mission, we recognize that we will encounter unique and novel issues related to privacy and handling of sensitive data. We will always treat victims with dignity and respect, protecting their privacy and data, and rigorously adhering to the U.S. Constitution, applicable laws, regulations, and policies, and the FBI's Core Values.

**Unique Authorities**. The FBI uses criminal and counterintelligence authorities to combat cyber criminals and foreign actors who use global infrastructure to compromise US networks.

> **Leading Cyber Threat Response**. The FBI leads the U.S. Government's response to significant cyber incidents by investigating, collecting evidence and intelligence, identifying additional victims, and pursuing disruption opportunities.
>
> **Using Law Enforcement Authorities to Have Broad Impact**. Computer intrusion is a crime, whether it's done for personal profit or on behalf of a foreign government. The FBI uses legal process to obtain evidence that enables FBI and partner agencies to identify virtual infrastructure, shut down dark markets, expose adversaries' tools, and disrupt malicious activity.
>
> **Assembling the Domestic Intelligence Picture**. The FBI is the nation's lead domestic intelligence agency. FBI intelligence on cyber threats and intrusions into US networks helps identify those responsible—the first step towards holding them accountable.

**Coordinating Through the National Cyber Investigative Joint Task Force (NCIJTF)**. Led by the FBI, the NCIJTF brings together more than 30 co-located agencies from the Intelligence Community and law enforcement in threat-focused mission centers to synchronize actions against cyber adversaries for maximum impact.

**World-Class Capabilities**. The FBI adapts to cyber threats by using innovative investigative techniques, developing cutting-edge analytic tools, and recruiting the next generation of the cyber workforce.

**Recovering Assets to Assist Victims**. The Internet Crime Complaint Center (IC3)'s Recovery Asset Team culls through thousands of public complaints to assist victims in recovering hundreds of millions of dollars lost to cyber crime.

**Multidisciplinary Threat Teams**. Squads of cyber-trained Special Agents, Intelligence Analysts, Computer Scientists, Data Analysts, and Digital Operations Specialists in FBI offices nationwide engage, assess, investigate, and respond to cyber threats in their communities.

**Responding to Incidents with the Cyber Action Team**. The FBI's Cyber Action Team is a rapid response technical investigative team distributed nationally to deploy and provide technical assistance to assist in the most complex intrusions and cyber incidents.

**Enduring Partnerships**. The FBI uses our unique role not only to pursue our own actions but also to enable our partners to defend networks, attribute malicious activity, sanction bad behavior, and take the fight to adversaries overseas.

**Trust-Based Relationships**. With 56 U.S. field offices, hundreds of satellite offices, and liaisons around the world, the FBI has global reach that extends to our communities. The FBI works alongside the public and private sectors in unique hubs built on long-term relationships to share and act on threat information.

**Enabling Industry Action**. The FBI works with government, industry, and academia through nonprofit organizations like the National Cyber-Forensics and Training Alliance (NCFTA) and the National Defense Cyber Alliance (NDCA) to identify and disrupt cyber crime and national security threats.

**Serving as the Indispensable U.S. Government Partner**. While law enforcement and counterintelligence actions are at the core of the FBI's mission, we can more significantly impact the threat when we sequence and coordinate our actions with domestic and international partners. Our information, access, and relationships are not only for FBI use; they are resources for others to leverage**.**

**Cross-Border Partnerships to Address a Global Threat**. FBI Cyber Assistant Legal Attachés in countries around the world work closely with international counterparts to share information, coordinate action, and seek justice for victims of cyber crime.

Source: https://www.ic3.gov/Media/PDF/Y2020/PSA201008.pdf.

# V. 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 summary 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.

## B. Commander, USCYBERCOM Congressional Testimony

The following excerpt is from the *Statement of General Paul M. Nakasone, Commander United States Cyberspace Command, before the 117th Congress Senate Armed Services Committee* on 5 April 2022:

Let me begin by acknowledging the dedicated service of our Service members and civilians at USCYBERCOM. Their mission is to plan and execute global cyber operations, activities and missions to defend and advance national interests in collaboration with domestic and international partners across the full spectrum of competition and conflict. Our three lines of operation are to:

- Provide mission assurance for the Department of Defense by directing the security, operation and defense of Department of Defense Information Network (DODIN), including DoD's critical infrastructure;
- Help deter and defeat strategic threats to the United States and its national interests; and
- Assist Combatant Commanders to achieve their objectives in and through cyberspace.

U.S. Cyber Command directs operations through its components. These include the Cyber National Mission Force-Headquarters (CNMF-HQ), Joint Force Headquarters-DoD Information Network (JFHQ-DODIN, the commander for which is dual-hatted as the Director of the Defense Information Systems Agency) and Joint Task Force Ares. They work with our Joint Force headquarters elements, the commanders for which are dual-hatted with one of the Services' cyber components (Army Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/16th Air Force and Coast Guard Cyber Command). The Command currently comprises 133 teams across the Cyber Mission Force (CMF), approximately 6,000 Service members, including National Guard and Reserve personnel on active duty. The CMF is due to grow by 14 teams over the next five years.

USCYBERCOM is postured to execute its missions and meet both the nation's near-term and enduring strategic challenges in cyberspace. I shall address the Command's role in the crisis caused by Russia's invasion of Ukraine, and then speak to our preparedness for persistent threats and in meeting our long-term pacing challenge, China. As the Commander of USCYBERCOM and Director of the National Security Agency (NSA), I have learned that the Command's linkage with NSA is essential to achieving critical outcomes for the nation in both cyber and intelligence operations. The dual-hatted command relationship improves planning, resource allocation, risk mitigation, and unity of effort. It allows us to operate with speed, agility, and mission effectiveness that we could not achieve without it. This is critical to meeting the strategic challenges of our adversaries as they grow in sophistication, aggressiveness and scope of operations.

*Strategic Challenges*

Russia's invasion of Ukraine demonstrated Moscow's determination to violate Ukraine's sovereignty and territorial integrity, forcibly impose its will on its neighbors and challenge the North Atlantic Treaty Organization (NATO). Russia's military and intelligence forces are employing a range of cyber capabilities, to include espionage, influence and attack units, to support its invasion and to defend Russian actions with a worldwide propaganda campaign.

U.S. Cyber Command (with NSA) has been integral to the nation's response to this crisis since Russian forces began deploying on Ukraine's borders last fall. We have provided intelligence on the building threat, helped to warn U.S. government and industry to tighten security within critical infrastructure sectors, enhanced resilience on the DODIN (especially in Europe),

accelerated efforts against criminal cyber enterprises and, together with interagency members, Allies, and partners, planned for a range of contingencies. Coordinating with the Ukrainians in an effort to help them harden their networks, we deployed a hunt team who sat side-by-side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine. In addition, USCYBERCOM is proactively ensuring the security and availability of strategic command and control and other systems across the Department. We have also crafted options for national decision makers and are conducting operations as directed.

When Moscow ordered the invasion in late February, we stepped up an already high operational tempo. We have been conducting additional hunt forward operations to identify network vulnerabilities. These operations have bolstered the resilience of Ukraine and our NATO Allies and partners. We provided remote analytic support to Ukraine and conducted network defense activities aligned to critical networks from outside Ukraine – directly in support of mission partners. In conjunction with interagency, private sector and Allied partners, we are collaborating to mitigate threats to domestic and overseas systems.

These measures were made possible by the patient investments in cyberspace operations capabilities and capacity over the last decade, as well as by the lessons that we as a Department and a nation have learned from operational experience. The current crisis is not over, but I am proud of the response of our people and confident in their ability to deliver results no matter how long it lasts. Their grit and ingenuity have been inspiring.

Shifting to longer-term considerations, I note that our operations are planned and executed in accord with the Interim National Security Strategic Guidance. Underpinning our work is Integrated Deterrence. We provide combat-capable forces in cyberspace that engage in active campaigning to disrupt adversary actions, demonstrate capabilities and resolve, shape adversary perceptions and gain warfighting advantages should deterrence fail. Integrated Deterrence is multi-partner, multi-domain, multi-theater and multi-spectrum, requiring us to compete every day in cyberspace against military and intelligence actors seeking to undermine our nation's strength and strategic advantages.

Cyberspace is a dynamic and inter-connected domain where near-peer adversaries seek to exploit gaps and seams between our organizations and authorities. Such adversaries use a variety of cyber means to compromise our systems, distort narratives and disseminate misinformation. These actions threaten our national interests by impairing the safety and security of our citizens, stealing intellectual property and personal information while seeking to undermine the legitimacy of our institutions. Our adversaries have demonstrated sophisticated cyber-attack capabilities for use in competition, crisis and conflict, but I am confident that USCYBERCOM is well postured to meet those challenges.

China is our pacing challenge, which I see as both a sprint and a marathon. China's military modernization over the past several years threatens to erode deterrence in the western Pacific, which requires immediate steps to redress. At the same time, China is an enduring strategic challenge that is now global in scope. Beijing is exerting influence worldwide through its rising diplomatic, informational, military, and economic power. China is a challenge unlike any other we have faced. I have therefore created a China Outcomes Group under joint USCYBERCOM and NSA leadership to ensure proper focus, resourcing, planning, and operations to meet this challenge. Although we recognize that much of our effort will be in support of U.S. Indo-Pacific Command, China is a global challenge. The success of our efforts will depend in part on the resilience and capabilities of regional and worldwide partners. We are building operating relationships and also dedicating long-term work to enhance their cybersecurity and cyberspace operations forces.

Iran and North Korea are cyber adversaries growing in sophistication and willingness to act. Despite our strengthened focus on China, we are maintaining our ability to counter these threats. Tehran has increased ransomware operations, the targeting of critical infrastructure, and influence campaigns (including in our 2020 elections). We support U.S. Central Command in its efforts against Iranian-backed proxies in Iraq and Syria (as we also did in the withdrawal from Afghanistan last summer). North Korea uses its cyber actors to generate revenue through criminal enterprises, such as hacking-for-hire and theft of cryptocurrency. USCYBERCOM works with the Departments of State and Treasury to stem Pyongyang's campaigns.

The scope, scale and sophistication of these threats is rising. The United States faced major cybersecurity challenges over the last year, beginning with the SolarWinds supply-chain compromise but extending to incidents involving software compromises that affected companies like Colonial Pipeline, Microsoft, JBS, Kaseya, and Apache. In each instance, our Command worked through CNMF and other components to provide insights to our homeland security and law enforcement partners, who are the nation's first line of defense for U.S. systems and networks.

Ransomware can have strategic effects as America saw in the disruption of Colonial Pipeline's systems. CNMF has taken numerous actions over the past year to combat ransomware in close partnership with law enforcement, interagency, industry, and foreign partners to disrupt and degrade the operations of ransomware groups attacking our nation's critical infrastructure. CNMF and NSA enabled whole-of-government actions targeting ransomware actors, passing key insights in near-real time. CNMF was a key partner in the whole-of- government effort to disrupt and impose costs against those who targeted Colonial Pipeline.

USCYBERCOM (with JFHQ-DODIN) also defended the DODIN against cyber threats and helped ensure that disruptions to its systems and data remained inconsequential and brief. We continue to innovate in enhancing DODIN defenses and countering adversary threats; indeed, we must, because our adversaries are agile and adaptive. Key to this effort is building resilience in our systems and platforms while preparing the Department, the other Combatant Commands and Defense Industrial Base (DIB) companies to operate even in degraded cyber environments.

*U.S. Cyber Command Posture for the Future*

Our success against these growing challenges is a result of sustained efforts and investments, not to mention a lot of hard work. I should add that that work over the last two years took place under COVID-19 mitigations. USCYBERCOM has been on-mission, running operations and exercises with the joint force and domestic and foreign partners throughout the pandemic, with negligible workforce transmission and slight impact to operations. We will continue to prioritize workplace safety, workforce confidence, and mission continuity.

We see 2022 as a year of opportunity to make progress in several areas that will enhance USCYBERCOM's capabilities and contributions to national security. With this in mind, I have established the following priorities for our Command:

- Readiness;
- Operations in Defense of the Nation;
- Integrated Deterrence;
- Recruiting, Retention and Training; and
- Joint Cyber Warfighting Architecture and Enhanced Budget Control

Readiness is priority one. It is foundational to the success of operations in defense of the nation and Integrated Deterrence. USCYBERCOM has made progress despite challenges. We

improved our ability to monitor the status of our cyber mission forces down to the team, mission element and individual levels. Across the Department, USCYBERCOM is responsible for setting standards for all of DoD's Cyberspace Operations Forces. We work to provide commanders with the situational awareness they require to assess risks and make informed decisions, not just in operations but in maintaining force readiness as a whole. We will work with the Services this year to ensure the progress we have made over the past year continues.

Second, along with our interagency partners, we defended the nation's recent elections against foreign interference and are preparing to support the defense of this year's midterms through the combined efforts of USCYBERCOM and NSA. We anticipate that our adversaries will continue using their military and intelligence elements to affect our democracy. Thus I appointed a USCYBERCOM general officer and an NSA senior executive to oversee election security in 2022. This is an enduring, no-fail mission for USCYBERCOM.

Interagency partnerships are crucial in these efforts. Working with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has demonstrated that we are much stronger together. Indeed, no single agency can defend the nation on its own. USCYBERCOM imposes costs on threat actors and provides insights to domestic and foreign partners to mitigate and respond to malign activity, enabling each to act under its respective authorities. We will continue to collaborate with our domestic partners across the federal government and the states to share best practices and expertise.

Our adversaries also target our economy. DIB companies are on the frontlines in cyberspace and are constantly targeted by malicious cyber actors. Over the past year, we have deepened our relationships with private industry through voluntary information sharing. Since the nation's critical infrastructure and systems are largely in private hands, these relationships have directly enhanced our operations, in addition to the security of their commercial systems.

Third, supporting the national priority of Integrated Deterrence means preparing for crisis and conflict while campaigning in competition across the full spectrum of cyber operations. It also means building the strategic partnerships that enable the defense of U.S. systems and networks beyond the DODIN and the DIB. Our foreign partnerships begin with our "Five Eye" Allies – the United Kingdom, Canada, Australia and New Zealand. The circle of partnership has been enlarged in recent years as we enhanced existing relationships with allies and forged new ones with several nations, especially in Europe and the Indo-Pacific region.

Fourth is building a skilled workforce through recruitment, training, and retention. Talent is key to preserving our competitive edge against our adversaries. USCYBERCOM has improved its civilian hiring with the use of its congressionally-granted Cyber Excepted Service (CES) authorities, which allow us to offer competitive compensation packages for high-demand expertise. In addition, a diverse, talented workforce that expands equity and inclusiveness is an enduring goal. To recruit and retain a skilled military workforce, we are also grateful for the authorities Congress has granted the Services to offer flexible promotion and commissioning avenues in support of the CMF.

Partnerships with academia will aid in engaging the future cyber workforce and enriching the strategic dialogue about cyber. Our new Academic Engagement network began last year and comprises 93 institutions, including 10 minority-serving institutions, across 40 states and the District of Columbia, as of March 25, 2022. Interest in partnering with USCYBERCOM is strong and growing.

Training and proficiency are improving through our mission simulation capabilities, particularly the Persistent Cyber Training Environment (PCTE). The PCTE is helping us mature cyber

operations tradecraft, enhance individual proficiencies and enable faster attainment of team certification and collective training in maneuvers such as Exercise CYBER FLAG.

The Reserve Component is critical to protecting the nation in cyberspace. As a result of the partnership between USCYBERCOM and the National Guard Bureau during the 2020 election, Guard units could rapidly share information on malicious cyber activity with state and local authorities. Members of the National Guard and Reserve often have private-sector experience in fields of strong interest to USCYBERCOM. In addition, the ability of the National Guard and Reserve to hire cyber talent has been especially helpful in retaining the contributions of Service members who decide to leave active duty upon completion of their commitment; members can transfer to a part-time status.

Our final priority is guiding the Department's investments in cyberspace capability through the Joint Cyber Warfighting Architecture (JCWA) and Enhanced Budget Control. JCWA consolidates and standardizes the Department's cyberspace operations capabilities, enabling us to integrate data from missions and monitoring to help commanders gauge risk, make timely decisions and act against threats at speed and scale. The Department is building JCWA and advancing the Cyber Mission Force's capabilities for conducting the full spectrum of cyberspace operations.

USCYBERCOM is grateful to this Committee and Congress for granting us Enhanced Budget Control over resources dedicated to the Cyber Mission Force. With this authority, USCYBERCOM will improve direction, control and synchronization of investments for cyber operations across the Department of Defense.

*Conclusion*

U.S. Cyber Command views 2022 as a year of significant opportunity for building our capabilities against the five priorities above. Our overarching goal is to build a Command that is ready and capable at providing options and conducting operations in defense of the nation with wider partnerships and world-class talent, all linked through the Joint Cyber Warfighting Architecture. These elements will be essential to our nation's security as it faces an array of adversaries who are expanding the scope, scale and sophistication of their operations against us, and will be critical to developing the right mission posture to meet the unprecedented challenge of China.

The men and women at U.S. Cyber Command are grateful for the support this Committee has given to our Command. We can only succeed with a strong partnership with Congress.

Source: https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/.

# VI. U.S. Cyber Law Guidance

## A. DOS 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.

## B. DOD Domestic and International Cyber Law Considerations

The following is an excerpt from a speech by Paul C. Ney, Jr., DOD General Counsel, at the U.S. Cyber Command Legal Conference on 2 March 2020 https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/DOD-general-counsel-remarks-at-us-cyber-command-legal-conference/:

**DOD General Counsel Remarks at U.S. Cyber Command Legal Conference**

I have two objectives today. First, I'll offer a snapshot of how we in DOD are integrating cyberspace into our overall national defense strategy. Second, I will summarize the domestic and international law considerations that inform the legal reviews that DOD lawyers conduct as part of the review and approval process for military cyber operations. We at DOD now have considerable practice advising on such operations and are accordingly in a position to begin to speak from experience to some of the challenging legal issues that cyber operations present.

To set the scene, when I talk about "cyberspace," I am referring to "the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Physically, and logically, the domain is in a state of perpetual transformation. It enables the transmission of data across international boundaries in nanoseconds – controlled much more by individuals or even machines than by governments – spreading ideas to disparate audiences and, in some cases, the generating of physical effects in far-flung places.

### 1. Today's Cyber Threat Environment and DOD's Response

As we enter the third decade of the twenty-first century, people are imagining, developing, and creating new technologies and devices at a faster rate than ever before. These new technologies update on a near daily basis – think of the software update that your phone automatically uploaded today.

Sophisticated technologies are now a part of nearly all aspects of military operations, creating opportunities and challenges. A recent Brookings paper makes the point well:

By … building Achilles' heels into everything they operate, modern militaries have created huge opportunities for their potential enemies. The fact that everyone is vulnerable … is no guarantee of protection.

Constantly changing vulnerabilities exist not only within our Armed Forces but also in the private and public sectors, which provide critical support to our operations. This includes contractors that manage networks and other services; the defense industrial base that is the foundation of the United States' military strength; and critical public infrastructure upon which the entire country, including the Armed Forces, relies for water, electricity, and transportation.

From a strategic competition perspective, too, cyberspace is increasingly dynamic and contested, including as a warfighting domain. In the past few years, other nations, in part to make up for gaps in conventional military power vis-à-vis the United States, have developed cyber strategies and organized military forces to conduct operations in cyberspace. China's Strategic Support Force, for example, provides its People's Liberation Army with cyberwarfare capabilities to "establish information dominance in the early stages of a conflict to constrain [U.S.] actions … by targeting network-based [command and control] … logistics, and commercial activities." Russia consistently uses cyber capabilities for what it calls "information confrontation" during peacetime and war. All of this is unsurprising because cyber is a relatively cheap form of gaining real power, especially for impoverished adversaries like North Korea: a cyber operation can require nothing more than a reasonably skilled operator, a computer, a network connection, and persistence.

A key element of the U.S. military's strategy in the face of these cyber-threats is to "defend forward." Implementing this element of the strategy begins with "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver" – which we refer to as "persistent engagement." "Persistent engagement recognizes that cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace." As General Nakasone has said, "[i]f we find ourselves defending inside our own networks, we have lost the initiative and the advantage." In short, the strategy envisions that our military cyber forces will be conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to U.S. national interests.

Cyber operations are also becoming an integral part of other military operations. As the 2018 National Defense Strategy emphasizes, "[s]uccess no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting." For example, during operations in Iraq in 2017, U.S. forces used cyber and space capabilities to disrupt communications to and from the enemy's primary command post, forcing the enemy to move to previously unknown backup sites, thereby exposing their entire command-and-control network to U.S. kinetic strikes. Operations like this will become increasingly common.

Because of the complexity and dynamism of the domain and the threat environment, the need for persistent engagement outside U.S. networks, and the critical advantage that cyber operations provide our Armed Forces, DOD must develop, review, and approve military cyber operations at so-called "warp-speed." To this end, the U.S. Government has made meaningful strides. You heard in 2018 that the President had issued National Security Presidential Memorandum-13, United States Cyber Operations Policy, or "NSPM-13" for short, which allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace. Congress also has clarified that the President has authority to direct military operations in cyberspace to counter adversary cyber operations against our national interests and that such operations, whether they amount to the conduct of hostilities or not, and even when conducted in secret, are to be considered traditional military activities and not covert action, for purposes of the covert action statute.

Even as the United States takes action to secure its vital national interests and to support its Allies and partners in this complex environment, it is a Nation dedicated to the rule of law. Consequently, we must ensure that our efforts are not only effective but also consistent with law and wider U.S. Government efforts to promote stability in cyberspace and adherence to the rules-based international order. DOD lawyers have an important role to play as the Department develops and executes cyber operations to meet these mandates.

Let me turn now to providing you a sense of how DOD lawyers analyze proposed military cyber operations for compliance with domestic and international law.

## 2. Framework for Legal Analysis

To evaluate the legal sufficiency of a proposed military cyber operation, we employ a process similar to the one we use to assess non-cyber operations. We engage our clients to understand the relevant operational details: What is the military objective we seek to achieve? What is the operational scheme of maneuver and how does it contribute to achieving that objective? Where is the target located? Does the operation involve multiple geographic locations? What is the target system used for? How will we access it? What effects – such as loss of access to data – will we generate within that system? How will those effects impact the system's functioning? Which people or processes will be affected by anticipated changes to the system's functioning? Are any of those likely to be impacted civilians or public services? Answers to these questions will drive the legal analysis.

### A. U.S. Domestic Law

Let's take up considerations of U.S. domestic law first. We begin with the foundational question of domestic legal authority to conduct a military cyber operation. The domestic legal authority for the DOD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation. We assess whether a proposed cyber operation has been properly authorized using the analysis we apply to all other operations, including those that constitute use of force. The President has authority under Article II of the U.S. Constitution to direct the use of the Armed Forces to serve important national interests, and it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of "war" under the Constitution, triggering Congress's power to declare war. Furthermore, the Supreme Court has long affirmed the President's power to use force in defense of the nation and federal persons, property, and instrumentalities. Accordingly, the President has constitutional authority to order military cyber operations even if they amount to use of force in defense of the United States. Of course, the vast majority of military operations in cyberspace do not rise to the level of a use of force; but we begin analysis of U.S. domestic law with the same starting point of identifying the legal authority.

In the context of cyber operations, the President does not need to rely solely on his Article II powers because Congress has provided for ample authorization. As I noted earlier, Congress has specifically affirmed the President's authority to direct DOD to conduct military operations in cyberspace. Moreover, cyber operations against specific targets are logically encompassed within broad statutory authorizations to the President to use force, like the 2001 Authorization for the Use of Military Force, which authorizes the President to use "all necessary and appropriate force" against those he determines were involved in the 9/11 attacks or that harbored them. Congress has also expressed support for the conduct of military cyber operations to defend the nation against Russian, Chinese, North Korean, and Iranian "active, systematic, and ongoing campaigns of attacks" against U.S. interests, including attempts to influence U.S. elections.

In addition to questions of legal authority, DOD lawyers advise on the Secretary of Defense's authority to direct the execution of military cyber operations as authorized by the President and statute, "including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power," and to conduct related intelligence activities. Our lawyers ensure that U.S. military cyber operations adhere to the President's specific authorizations as well as the generally applicable NSPM-13.

After concluding that the operation has been properly authorized, DOD lawyers assess whether there are any statutes that may restrict DOD's ability to conduct the proposed cyber operation and whether the operation may be carried out consistent with the protections afforded to the privacy and civil liberties of U.S. persons. To illustrate, I am going to talk about two statutes and the First Amendment as examples of laws that we may consider, depending on the specific cyber operation to be conducted.

First, let's look at federal criminal provisions in Title 18 of the U.S. Code that prohibit accessing certain computers and computer networks "without authorization" or transmitting a "program, information, code, or command" that intentionally causes "any impairment to the integrity or availability" of the computer or data on it – provisions found in the Computer Fraud and Abuse Act or "CFAA," as amended. These provisions contain exceptions for lawfully authorized activities of law enforcement agencies and U.S. intelligence agencies but do not refer to U.S. military cyber operations. Common sense and long-accepted canons of statutory interpretation suggest, however, that the CFAA will not constrain appropriately authorized DOD cyber operations.

The CFAA was enacted to protect U.S. Government computers and critical banking networks against thieves and hackers, not vice versa; it expresses no clear indication of congressional intent to limit the President from directing military actions; and the more recent statutes I mentioned earlier specifically authorize or reaffirm the President's authority to direct DOD to conduct operations in cyberspace. In light of these considerations, it would be unreasonable and counterintuitive to interpret the CFAA as restricting properly authorized military cyber operations abroad against foreign actors.

Second, DOD lawyers typically analyze whether the proposed cyber operation may be conducted as a traditional military activity – or "TMA" – such that it would be excluded from the approval and oversight requirements applicable to covert action under the Covert Action Statute. Because the statute does not define TMA, we look to the legislative history and a provision in the National Defense Authorization Act for Fiscal Year 2019 that clarifies that in general clandestine military activities in cyberspace constitute TMA for purposes of the Covert Action Statute, and reaffirms established congressional reporting requirements for military cyber operations.

Third, DOD lawyers must assess whether a proposed operation will impact the privacy and civil liberties of U.S. persons. The practical reality of cyberspace today is that U.S. military cyber operations aimed at disrupting an adversary's ability to put information online or to distribute it across the worldwide web have the potential to affect U.S. persons' rights and civil liberties in ways that operations in physical domains do not.

Let me give you a concrete example. A core part of DOD's mission to defend U.S. elections consists of defending against covert foreign government malign influence operations targeting the U.S. electorate. The bulk of DOD's efforts in this area involve information-sharing and support to domestic partners, like the Department of Homeland Security and the Federal Bureau of Investigation. But what about a U.S. military cyber operation to disrupt a foreign government's ability to disseminate covertly information to U.S. audiences via the Internet by pretending that the information has been authored by Americans inside the United States? Can we conduct such an operation in a manner that contributes to the defense of our elections but avoids impermissible interference with the right of free expression under the First Amendment – including the right to receive information? The analysis often turns on the specifics of the proposed operation – but, in short, we believe we can.

Few precedents address this issue directly; but, U.S. case law does provide a framework with at least three key strands. First, there are judicial decisions that stand for the proposition that the U.S. Government, in carrying out certain appropriately authorized activities, may incidentally burden the right to receive information from foreign sources without violating the First Amendment. Second, courts have recognized a compelling government interest in protecting U.S. elections from certain types of foreign influence – especially when that influence is exercised covertly. Third, government action based on the content of the speech will be suspect.

In light of these precedents, DOD lawyers analyzing particular cyber operations for First Amendment compliance will consider a number of factors, including: whether the operation is targeting the foreign actors seeking to influence U.S. elections covertly rather than the information itself; the extent to which the operation may be conducted in a "content neutral" manner; and, the foreign location and foreign government affiliation of the targeted entity.

We at DOD realize that military involvement in protecting U.S. elections is a sensitive mission, even when conducted in compliance with First Amendment protections and consistent with congressional intent. Virtually any military involvement in U.S. elections implicates the bedrock premise of maintaining civilian control of the military and our long tradition of keeping the military out of domestic politics. Accordingly, in assessing proposed operations related to elections,

DOD lawyers pay particular attention to whether the proposed operation may be conducted consistent with legal and regulatory limits on the use of official positions to influence or affect the results of U.S. elections or to engage in, or create the appearance of engaging in, partisan politics.

**B. International Law**

Those are some highlights of U.S. domestic law considerations that may be implicated by proposed military cyber operations; let me turn now to international law.

We recognize that State practice in cyberspace is evolving. As lawyers operating in this area, we pay close attention to States' explanations of their own practice, how they are applying treaty rules and customary international law to State activities in cyberspace, and how States address matters where the law is unsettled. DOD lawyers, and our clients, engage with our counterparts in other U.S. Government departments and agencies on these issues, and with Allies and partners at every level – from the halls of the United Nations to the floors of combined tactical operations centers – to understand how we each apply international law to operations in cyberspace. Initiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make. My intent here is not to lay out a comprehensive set of positions on international law. Rather, as I have done with respect to domestic law, I will tell you how DOD lawyers address some of the international law issues that today's military cyber operations present.

I will start with some basics. It continues to be the view of the United States that existing international law applies to State conduct in cyberspace. Particularly relevant for military operations are the Charter of the United Nations, the law of State responsibility, and the law of war. To determine whether a rule of customary international law has emerged with respect to certain State activities in cyberspace, we look for sufficient State practice over time, coupled with opinio juris – evidence or indications that the practice was undertaken out of a sense that it was legally compelled, not out of a sense of policy prudence or moral obligation.

As I discussed a few minutes ago, our policy leaders assess that the threat environment demands action today – our clients need our advice today on how international legal rules apply when resorting to action to defend our national interests from malicious activity in cyberspace, notwithstanding any lack of agreement among States on how such rules apply. Consequently, in reviewing particular operations, DOD lawyers provide advice guided by how existing rules apply to activities in other domains, while considering the unique, and frequently changing, aspects of cyberspace.

First, let's discuss the international law applicable to uses of force. Article 2(4) of the Charter of the United Nations provides that "All 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." At the same time, international law recognizes that there are exceptions to this rule. For example, in the exercise of its inherent right of self-defense a State may use force that is necessary and proportionate to respond to an actual or imminent armed attack. This is true in the cyber context just as in any other context.

Depending on the circumstances, a military cyber operation may constitute a use of force within the meaning of Article 2(4) of the U.N. Charter and customary international law. In assessing whether a particular cyber operation – conducted by or against the United States – constitutes a use of force, DOD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine. Even if a particular cyber operation does not constitute a use of force, it is important to keep in mind that the State or States targeted by the operation may disagree, or at least have a different perception of what the operation entailed.

Second, the international law prohibition on coercively intervening in the core functions of another State (such as the choice of political, economic, or cultural system) applies to State conduct in cyberspace. For example, "a cyber operation by a State that interferes with another country's ability to hold an election" or that tampers with "another country's election results would be a clear violation of the rule of non-intervention." Other States have indicated that they would view operations that disrupt the fundamental operation of a legislative body or that would destabilize their financial system as prohibited interventions.

There is no international consensus among States on the precise scope or reach of the non-intervention principle, even outside the context of cyber operations. Because States take different views on this question, DOD lawyers examining any proposed cyber operations must tread carefully, even if only a few States have taken the position publicly that the proposed activities would amount to a prohibited intervention.

Some situations compel us to take into consideration whether the States involved have consented to the proposed operation. Because the principle of non-intervention prohibits "actions designed to coerce a State … in contravention of its rights," it does not prohibit actions to which a State voluntarily consents, provided the conduct remains within the limits of the consent given.

Depending on the circumstances, DOD lawyers may also consider whether an operation that does not constitute a use of force could be conducted as a countermeasure. In general, countermeasures are available in response to an internationally wrongful act attributed to a State. In the traditional view, the use of countermeasures must be preceded by notice to the offending State, though we note that there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency. In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a State within the timeframe in which the DOD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available.

For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory. This proposition is recognized in the Department's adoption of the "defend forward" strategy: "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The Department's commitment to defend forward including to counter foreign cyber activity targeting the United States – comports with our obligations under international law and our commitment to the rules-based international order.

The DOD OGC view, which we have applied in legal reviews of military cyber operations to date, shares similarities with the view expressed by the U.K. Government in 2018. We recognize that there are differences of opinion among States, which suggests that State practice and opinio juris are presently not settled on this issue. Indeed, many States' public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations (regardless of whatever penalties may be imposed under domestic law).

Traditional espionage may also be a useful analogue to consider. Many of the techniques and even the objectives of intelligence and counterintelligence operations are similar to those used in cyber operations. Of course, most countries, including the United States, have domestic laws against espionage, but international law, in our view, does not prohibit espionage per se even

when it involves some degree of physical or virtual intrusion into foreign territory. There is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it. In examining a proposed military cyber operation, we may therefore consider the extent to which the operation resembles or amounts to the type of intelligence or counterintelligence activity for which there is no per se international legal prohibition.

Of course, as with domestic law considerations, establishing that a proposed cyber operation does not violate the prohibitions on the use of force and coercive intervention does not end the inquiry. These cyber operations are subject to a number of other legal and normative considerations.

As a threshold matter, in analyzing proposed cyber operations, DOD lawyers take into account the principle of State sovereignty. States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.

It is also longstanding DOD policy that U.S. forces will comply with the law of war "during all armed conflicts however such conflicts are characterized and in all other military operations." Even if the law of war does not technically apply because the proposed military cyber operation would not take place in the context of armed conflict, DOD nonetheless applies law-of-war principles. This means that the jus in bello principles, such as military necessity, proportionality, and distinction, continue to guide the planning and execution of military cyber operations, even outside the context of armed conflict.

DOD lawyers also advise on how a proposed cyber operation may implicate U.S. efforts to promote certain policy norms for responsible State behavior in cyberspace, such as the norm relating to activities targeting critical infrastructure. These norms are non-binding and identifying the best methods for integrating them into tactical-level operations remains a work in progress. But, they are important political commitments by States that can help to prevent miscalculation and conflict escalation in cyberspace. DOD OGC, along with other DOD leaders, actively supports U.S. State Department-led initiatives to build and promote this framework for responsible State behavior in cyberspace. This includes participation in the UN Group of Governmental Experts and an Open-Ended Working Group on information and communications technologies in the context of international peace and security. These diplomatic engagements are an important part of the United States' overall effort to protect U.S. national interests by promoting stability in cyberspace.

Of course, the real work of analyzing specific military cyber operations in light of the domestic and international legal considerations I have mentioned falls to judge advocates and civilian attorneys at the tactical and operational levels – which is to say, many of you. As one of my predecessors, Jennifer O'Connor, noted in a speech in 2016, military operations – including cyber operations – are subject to a rigorous targeting process that involves both policy and legal reviews to ensure that specific operations are conducted consistent with the relevant authorization, domestic and international law, and any additional restraints imposed by the applicable orders. Particularly in areas like this one, in which not only the law but the domain itself is constantly evolving, I am extremely proud of the legal work many of you do for the Department of Defense and am humbled every day by your dedication to our Nation's defense.

Source: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/DOD-general-counsel-remarks-at-us-cyber-command-legal-conference/.

## C. 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://DOD.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://DOD.defense.gov/Portals/1/Documents/pubs/DOD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

# Appendix B: U.S. Cyberspace Organizations

**Appendix B includes:**

I. **Department of State**
   - **Bureau of Cyberspace and Digital Policy (CDP)**

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

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

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

V. **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 / 16th Air Force**
   - **Coast Guard Cyber**

## I. Department of State – Bureau of Cyberspace and Digital Policy (CDP)

Ensuring the security of cyberspace is fundamental to protecting America's national security and promoting the prosperity of the American people. Cyberspace is an integral component of all facets of American life, including the country's economy and defense. Yet private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities.

In partnership with other countries, the Department of State 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.

The Bureau of Cyberspace and Digital Policy (CDP) leads and coordinates the Department's work on cyberspace and digital diplomacy to encourage responsible state behavior in cyberspace and advance policies that protect the integrity and security of the infrastructure of the Internet, serve U.S. interests, promote competitiveness, and uphold democratic values.

- The Bureau addresses the national security challenges, economic opportunities, and values considerations presented by cyberspace, digital technologies, and digital policy and promotes standards and norms that are fair, transparent, and support our values.
- The CDP bureau includes three policy units: International Cyberspace Security, International Information and Communications Policy, and Digital Freedom.

Sources: https://www.state.gov/policy-issues/cyber-issues/ and https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/.

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

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

**Designed for Collaboration and Partnership**. Established in 2018, CISA was created to work across public and private sectors, challenging traditional ways of doing business by engaging with government, industry, academic, and international partners. As threats continue to evolve, we know that no single organization or entity has all the answers for how to address cyber and physical threats to critical infrastructure. By bringing together our insight and capabilities, we can build a collective defense against the threats we face.

**Mission**. Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.

**Vision**. A secure and resilient critical infrastructure for the American people

**CISA Plays Two Key Roles**.

1. Operational Lead for Federal Cybersecurity, or the Federal "dot gov".
    - CISA acts as the quarterback for the federal cybersecurity team, protecting and defending the home front – our federal civilian government networks – in close partnership with the Office of Management and Budget, which is responsible federal cyber security overall. CISA also coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners.
2. National Coordinator for Critical Infrastructure Security and Resilience.
    - We look at the entire threat picture and work with partners across government and industry to defend against today's threats while securing the nation's critical infrastructure against threats that are just over the horizon.

Source: https://www.cisa.gov/about-cisa.

## III. Department of Defense

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

**Mission**. The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) insights and cybersecurity products and services and enables computer network operations to gain a decisive advantage for the nation and our allies.

> The **Central Security Service (CSS)** provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community, while promoting partnership between the NSA and the cryptologic elements of the Armed Forces.

**Combat Support**

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. NSA analysts, linguists, engineers and other personnel deploy to Afghanistan and other hostile areas to provide actionable SIGINT and cybersecurity support to warfighters on the front lines.

We provide intelligence support to military operations through our signals intelligence activities, while our cybersecurity 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 cybersecurity 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.

**Signals Intelligence (SIGINT)**. NSA is responsible for providing foreign signals intelligence (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 that provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

Our 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.

At NSA, we must keep pace with advances in the high-speed, multifunctional technologies of today's information age. The ever-increasing volume, velocity and variety of current signals make the production of relevant and timely intelligence for military commanders and national policy-makers more challenging and exciting than ever. Modern telecommunications technology poses significant challenges to the SIGINT mission, and many languages are used around the world that are of interest to our military and national leaders. Thus, NSA is required to maintain a wide variety of language capabilities as well. Successful SIGINT depends on the skills of language professionals, mathematicians, analysts, and engineers, to name just a few.

The critical thinking and vitality required to accomplish our strategic goals depend on a diverse workforce, divergent points of view, and a fully-inclusive environment. NSA has a strong

tradition of employing dedicated, highly-qualified people who are deeply committed to maintaining the nation's security. While technology will obviously continue to be a key element of our future, NSA recognizes that technology is only as good as the people creating it and the people using it.

**Cybersecurity**. NSA Cybersecurity prevents and eradicates threats to U.S. national security systems with a focus on the Defense Industrial Base and the improvement of our weapons' security. Through our Cybersecurity Collaboration Center, NSA partners with allies, industry and researchers to strengthen awareness to advance cybersecurity outcomes.

> **Cybersecurity Collaboration Center**. NSA's Cybersecurity Collaboration Center harnesses the power of industry partnerships to prevent and eradicate foreign cyber threats to National Security Systems (NSS), the Department of Defense, and the Defense Industrial Base (DIB). This groundbreaking hub for engagement with the private sector is designed to create an environment for information sharing between NSA and its partners combining our respective expertise, techniques, and capabilities to secure the nation's most critical networks.

Sources: https://www.nsa.gov/about/.

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

The DoD CIO is the principal staff assistant and senior advisor to the Secretary of Defense and Deputy Secretary of Defense for information technology (IT) (including national security systems and defense business systems), information resources management (IRM), and efficiencies. This means that DoD CIO is responsible for all matters relating to the DoD information enterprise, such as cybersecurity, communications, information systems, and more.

**Mission**. Protect. Connect. Perform.

**Vision**. To Deliver an Information Dominant Domain to Defeat our Nation's Adversaries

**Key Focus Areas**. Cloud, Communications, Cybersecurity, Enabling Artificial Intelligence, and Data.

DOD CIO includes the following organizations:

**Deputy Chief Information Officer for Command, Control, and Communications (DCIO C3)**. Provides expertise and broad guidance on policy, programmatic, and technical issues relating to C3 to integrate and synchronize DoD-wide communications and infrastructure programs and efforts to achieve and maintain information dominance for the Department.

DCIO C3 also manages efforts defining DoD policies and strategies for design, architecture, interoperability standards, capability development, and sustainment of critical C2 and communications for nuclear and non-nuclear strategic strike, integrated missile defense, and Defense and National Leadership Command Capabilities. Its sub organizations include Spectrum Policy and Programs; C3, including military and commercial SATCOM and Positioning, Navigation, and Timing; and National Leadership Command Capabilities.

This organization focuses on several DoD CIO top priorities, including empowering data access for DoD personnel through mobile devices and networks as well as sharing scarce spectrum resources with partners across industry and government. These efforts are critical to empowering secure, efficient, effective information technology for the Warfighter, because they look toward the future of accessing and utilizing information.

**Deputy Chief Information Officer for Cyber Security (DCIO CS)**. Provides expert policy, technical, program, and Defense-wide oversight on all aspects and matters related to DoD Cybersecurity. The office oversees the integration of Defense-wide programs to protect the Department's critical infrastructure against advanced persistent threats, and assures coordination of cybersecurity standards, policies, and procedures with other federal agencies, coalition partners, and industry. The DCIO CS priority is to support the Department's Cyber Strategy and DoD CIO's Vision to deliver an information dominant domain to defeat our Nation's adversaries. Policies and programs are designed to:

1. Ensure the Joint Force can achieve its missions in a contested cyberspace environment

2. Strengthen the Joint Force ability to conduct cyberspace operations that enhance U.S. military advantages

3. Supports the defense of U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident

4. Secure DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks

5. Expand DoD cyber cooperation with interagency, industry, and international partners.

**Deputy Chief Information Officer for Information Enterprise (DCIO IE)**. Establishes information technology (IT) policy and guidance for the infrastructure components of the DoD Information Enterprise to include networks, compute, and software. In this capacity, the DCIO IE organization oversees and manages ongoing enterprise IT capabilities as well as Department-wide modernization and reform initiatives. These capabilities and initiatives must enable the seamless and secure use of data to solidify an operational advantage, establish a more reliable and resilient IT foundation in support of a more mobile and remote workforce, and ensure the continued evolution of IT in a manner that is both mission impactful and fiscally responsible.

The organization executes critical activities to both maintain and modernize the DoD Information Enterprise. Among the activities covered are network optimization across Defense Agencies and DoD Field Activities, cloud and software modernization adoption across the Department, and better implementation of collaboration and productivity capabilities across the defense workforce. In partnership with the other DCIOs and DoD Components at large, the efforts of the DCIO IE team are foundational to achieving successful IT outcomes across a diverse range of operational missions and ensures that information remains one of our nation's greatest sources of power.

DCIO IE's directorates include DoD Information Network Modernization, focused on advancing DoD communications capabilities globally; Enterprise Capabilities, focused on driving adoption of proven infrastructure technologies (e.g., cloud and modern software development); and the Cloud Computing Program Office (CCPO), focused on the acquisition and execution of enterprise cloud programs.

As digital capabilities become increasingly critical in mission success, the DCIO IE organization will continue to press and act on priorities that ensure the Department's military edge.

**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.

DCIO R&A is the focal point for the Planning, Programming, Budgeting, and Execution (PPB&E) process, DoD CIO's congressional issues, and administration and management. Its sub organizations include Resource, Program, and Budget, which covers issues such as overseeing DoD IT & Cyberspace budget for the Office of Management and Budget and Congress; Administration and Management, which includes personnel management and congressional support; and Cyber Workforce which implements DoD efforts to transform the cyberspace workforce in support of U.S. national security priorities.

This organization underpins all of DoD CIO's priority areas by managing and overseeing the Department's IT & cyberspace budget to help the DoD CIO provide strategy, leadership, and guidance to create a unified information management and technology vision for the Department. This helps ensure that warfighters have the right IT/cyber, secure communications equipment, and capabilities that they need to execute their missions.

Sources: http://DODcio.defense.gov/ and http://DODcio.defense.gov/About-DOD-CIO/.

## C. Defense Information Systems Agency (DISA)

**Overview:** DISA is a combat support agency of the DOD. The agency is composed of more than 7,000 military and civilian employees and we provide, operate and assure command, control, information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders and other mission and coalition partners across the full spectrum of 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.

**DISA's Mission Partner Support:** 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.

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) DOD Information Network (DODIN), which maintains command and control (C2) of defensive cyber operations.

DISA delivers hundreds of IT support and service capabilities to our mission partners. These capabilities are captured in our online service catalog, https://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 nine unified combatant commands.

**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 JCS chairman and each of the service chiefs have endorsed JIE as a military imperative. The Deputy Management Action Group, a part of DCMO that considers department-wide management and business issues, has endorsed the JIE's viability to efficiently address budget issues, the threat vector and the need to be dominant in the information operations.

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. We have 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.

## IV. Joint Organizations

## A. U.S. Cyber Command (USCYBERCOM)

**Mission**: Direct, Synchronize, and Coordinate Cyberspace Planning and Operations – to Defend and Advance National Interests – in Collaboration with Domestic and International Partners

**Vision**: Achieve and maintain superiority in the cyberspace domain to influence adversary behavior, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests.

**Focus**: The Command has three main focus areas:

- Defending the DoDIN
- Providing support to combatant commanders for execution of their missions around the world
- 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 the military service cyber components.

- Army Cyber Command (ARCYBER)
- Fleet Cyber Command / Tenth Fleet (FLTCYBER)
- Sixteenth Air Force / Air Forces Cyber (AFCYBER)
- Marine Corps Forces Cyberspace Command (MARFORCYBER)

**Forces**: The Cyber Mission Force (CMF), authorized in 2012, originally consisted of 133 teams, with a total of almost 6,200 military and civilian personnel.

CMF teams come in several types:

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

**Combatant Command Support**. USCYBERCOM also aligned the Cyber Mission Force in support of Joint Force operations. CMF teams supported combatant commands under USCYBERCOM's Joint Force Headquarters:

- 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. Indo–Pacific Command (USINDOPACOM), U.S. Southern Command (USSOUTHCOM), and U.S. Space Command (USSPACECOM).
- AFCYBER supports U.S. European Command (USEUCOM), U.S. Strategic Command (USSTRATCOM), and U.S. Transportation Command (USTRANSCOM)

All 133 teams of the CMF achieved IOC in 2016, the threshold capacity whereby the units could execute their fundamental missions. The CMF reached Full Operational Capability (FOC) in 2018, when all CMF units had reached their projected full strength. At the time of the announcement, the CMF had about 5,000 military and civilian personnel across the 133 teams.

USCYBERCOM added two components:

- The Cyber National Mission Force (CNMF) in 2014. The CNMF is a joint element focused on cyberspace operations to deter, disrupt, and if necessary, defeat adversary cyber and malign influence actors.
- The Joint Force Headquarters–DoD Information Network (JFHQ-DoDIN) in 2015. JFHQ-DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses. The JFHQ-DoDIN commander is dual–hatted as the director of the Defense Information Systems Agency (DISA).
- USCYBERCOM added JTF-Ares to combat terrorist threats in 2016.

Sources: https://www.cybercom.mil/ and https://www.cybercom.mil/About/History/.

## B. Joint Spectrum Center (JSC)

**Vision**: Be the premier and trusted provider of enterprise electromagnetic spectrum tools, capabilities, services, data and applied engineering.

**Mission**: Provide direct support to the Joint Chiefs of Staff (JCS), Combatant Commands (CCMDs), and Military Departments (MILDEPs) to enable trusted, efficient and effective use of the Electromagnetic Spectrum Enterprise (operations, services, data, tools/capabilities), Applied Engineering, Acquisition and Analysis, and the mitigation of Electromagnetic Environmental Effects (E3) in support of our national security and military objectives.

**Mission Sets**:

- Direct Combatant Command and Joint Task Force Support
- Strategic Spectrum Planning – National and International
- Enterprise capabilities & services – Enables effective global spectrum operations and information dominance
- Engineering center of excellence – SME's, experience and tools required to address the complex technical and operational issues associated with spectrum operations and the mitigation of electromagnetic effects

**Lines of Effort**:

- **Operations**
  - Worldwide Deployable Spectrum Teams
  - On Call Joint Spectrum Interference Resolution (EMI)
  - Support to Information Ops/Special Technical Ops & Electronic Warfare
  - Hazards of Electromagnetic Radiation on Ordinance Mitigation
  - Electromagnetic Environment (EME) Analysis
  - Electromagnetic Compatibility (EMC) Analysis
  - Battlefield Training and Ops Support/Management
  - Joint Electromagnetic Operations & Visualization
  - Mobile Service Provider/FIRSTNet Support
- **Modeling and Simulation**
  - E3 Assessment & Spectrum Survivability/Supportability
  - DOD Equipment Acquisition & Test Assessments
  - EMS Battlefield Management Operation Picture
- **Database/Standards Development, Management & Maintenance**
  - Collect and maintain SM, E3, and HERO data
  - Develop DOD E3 technical standards
  - Operate and maintain the DOD Frequency Resource Record System (FRRS)
  - Manage the configuration and maintenance of SXXI
  - Parametric Data Integration & Distribution
- **Capability Development**
  - Global Electromagnetic Spectrum Information System (GEMSIS) Suite of Tools Development
  - Develop Spectrum E3 Modeling and Simulation Capabilities
  - Develop analytical E3 algorithms and tools to support spectrum operations, management and E3 Engineering
  - Research and efficiently/effectively integrate Spectrum technologies

Source:
https://storefront.disa.mil/kinetic/app/resources/disa/DSO%20JSC%20Overview%20brief.pdf
.

## C. Joint Communications Support Element (JCSE)

**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 CSD mission is to maintain trained and ready teams for worldwide deployment to plan organize, and direct the overall accomplishment of all levels of maintenance support of power generation, environmental control, and transportation assets assigned or attached to JCSE.
- 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.

# V. Service Organizations

## A. Army Cyber Command (ARCYBER)

U.S. Army Cyber Command (ARCYBER) is the Army headquarters beneath United States Cyber Command. ARCYBER operates and defends Army networks and delivers cyberspace effects against adversaries to defend the nation.

**Mission**. U.S. Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information dimension, while denying the same to our adversaries.

**Priorities**.

- Operate and aggressively defend the Department of Defense Information Network. This is our most critical and complex priority.
- Deliver cyberspace effects – both defensive and offensive – against global adversaries.
- Rapidly develop and deploy cyberspace capabilities to equip our force for the future fight against a resilient, adaptive adversary.

**Organization**. Army cyber units include:

**U.S. Army Network Enterprise Technology Command (NETCOM)** headquartered at Fort Huachuca, AZ, is the Army's single information technology service provider for all network communications.

A major subordinate command to U.S. Army Cyber Command, NETCOM leads global operations for the Army's portion of the DODIN, ensuring freedom of action in cyberspace while denying the same to our adversaries in support of multi-domain operations.

The command provides support to organizations across the entire spectrum of strategic, expeditionary, joint and combined environments.

**1st Information Operations Command (Land)**. is the Army's only Active Component Information Operations organization. A multi-component, brigade-level organization, it consists of a Headquarters and Headquarters Detachment (HHD) and two battalions. 1st IO Command's mission is to provide Information Operations and Cyberspace Operations support to the Army and other Military Forces through deployable teams, reach back planning and analysis, and specialized training.

**780th Military Intelligence Brigade (Cyber)** The brigade conducts cyberspace operations to deliver effects in support of Army and Joint requirements. It is a major subordinate command of INSCOM and is under OPCON of ARCYBER. The 780th MI Brigade is the only offensive cyberspace operations brigade in the U.S. Army and it actively fights alongside our Joint partners to achieve U.S. supremacy in an increasingly contested cyberspace and electromagnetic spectrum.

**Cyber Protection Brigade (CPB)** known as the Hunter Brigade, is the Army's premier cyber force. The CPB hunts against specified threats to deny and deter enemy offensive cyber operations. To do this, the CPB employs small teams of highly trained professionals operating in Mission Elements, supported by Analytic Support Cells, to hunt adversaries across the Army's Unified Network.

Source: http://www.arcyber.army.mil/.

## 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 (CDRUSCYBERCOM), 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.

- 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.
- Has direct operational control of Marine Corps Cyberspace Warfare Group (MCCYWG) and Marine Corps Cyberspace Operations Group (MCCOG) to support mission requirements and tasks. Additionally, the Marine Corps Information Operations Center (MCIOC) will be in direct support of MARFORCYBER for full spectrum cyber operations.

**MARFORCYBER Subordinate Units**.

1. Marine Corps Cyberspace Operations Group (MCCOG). MCCOG executes Marine Corps Department of Defense Information Network (DODIN) Operations and Marine Corps Defensive Cyberspace Operations (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. Key MCCOG tasks include:

- Provide Cyberspace Operations (CO) Support to Marine Air Ground Task Forces (MAGTFs)
- Plan and Direct Marine Corps Enterprise Network (MCEN) Operations
- Plan and Direct Defensive Cyberspace Operations (DCO)

2. Marine Corps Cyberspace Warfare Group (MCCYWG). MCCYWG organizes, trains, equips, provides administrative support, manages readiness of assigned forces, and recommends certification and presentation of Cyber Mission Force (CMF) Teams to U.S. Cyber Command. The MCCYWG plans and conducts full spectrum cyberspace operations as directed by COMMARFORCYBER in support of service, combatant command, joint, and coalition requirements. Key MCCYWG tasks include:

- Conduct personnel management to organize and assign individuals to work roles and place them in work centers to ensure operational readiness of CMF Teams
- Ensure all personnel are trained in accordance with USCYBERCOM Joint Cyberspace Training and Certification Standards and equipped to perform all duties and tasks outlined in the MARFORCYBER Mission Essential Task List (METL)
- Plan for and, when authorized, conduct OCO including computer network exploitation (CNE), cyberspace intelligence, surveillance, and reconnaissance (ISR) and operational preparation of the environment (OPE)

- Plan and conduct designated DCO in response to threats against the MCEN, supported combatant command (COCOM) designated networks, and the Department of Defense Information Network (DODIN)
- Advise COMMARFORCYBER on force employment considerations
- Provide subject matter expertise for operational planning requirements

Sources: https://www.marforcyber.marines.mil/ and https://www.marforcyber.marines.mil/About/.

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

U.S. Fleet Cyber Command (FCC)/U.S. TENTH Fleet (C10F) has grown into an operational force composed of more than 19,000 Active and Reserve Sailors and civilians organized into 26 active commands, 40 Cyber Mission Force units, and 29 reserve commands around the globe.

U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for Navy information network operations, offensive and defensive cyberspace operations, space operations and signals intelligence. As such, U.S. Fleet Cyber Command serves as the Navy component command to U.S. Cyber Command, the Navy space component to U.S. Strategic Command, and the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service. U.S. TENTH Fleet is the operational arm of Fleet Cyber Command and executes its mission through a task force structure similar to other warfare commanders. In this role, TENTH Fleet provides operational direction through the command's Maritime Operations Center located at Fort George Meade, MD.

### 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 US government, Department of Defense, 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 commands 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.

Sources: https://www.fcc.navy.mil/ and https://www.fcc.navy.mil/ABOUT-US/MISSION-VISION/.

## D. 16th Air Force / Air Forces Cyber (AFCYBER)

The Sixteenth Air Force (Air Forces Cyber) is headquartered at Joint Base San Antonio-Lackland, TX. Also known as the Air Force's Information Warfare Numbered Air Force, the 16th integrates multisource intelligence, surveillance, and reconnaissance, cyber warfare, electronic warfare, and information operations capabilities across the conflict continuum to ensure that our Air Force is fast, lethal and fully integrated in both competition and in war. Sixteenth Air Force (Air Forces Cyber) provides mission integration of IW at operational and tactical levels … recognizing the role of information in creating dilemmas for adversaries in competition and, if necessary, future conflicts.

**Mission**. Optimize and synchronize the readiness, generation, employment and presentation of cyberspace; electromagnetic spectrum; information; intelligence, surveillance, and reconnaissance; weather; and other related capabilities to generate information warfare outcomes for combatant commanders and air components.

**Vision**. Empowered Airmen delivering outcomes for the Nation

**Organization**. Sixteenth Air Force operates globally across nine wings and one center presenting capabilities to generate insights on our adversaries while simultaneously ensuring and having the capabilities and the capacity to persistently engage and respond appropriately to threats today, in the future, and across the competition continuum.

**Roles and Responsibilities**. The 16th Air Force commander has unique and distinct roles and responsibilities. 16th Air Force is responsible to:

- The Director, National Security Agency / Chief, Central Security Service, as the Air Force's authority for matters involving the conduct of cryptologic activities, including the spectrum of missions related to tactical war-fighting and national-level operations.
- The Office of the Under Secretary of Defense for Intelligence and Security, as a Defense Intelligence Component, for performing foreign intelligence missions and functions, and providing intelligence oversight of those missions and functions.
- Air Combat Command and the air components for organizing, training, and equipping; and force presentation of assigned forces.
- U.S. Cyber Command and the U.S. Air Force for building, extending, operating, securing, and defending the Air Force portion of the Department of Defense information network.
- U.S. Cyber Command as the Commander of Air Force Forces (COMAFFOR), for presentation of cyber forces to other cyber components as directed.
- U.S. Cyber Command, U.S. European Command, U.S. Space Command, and U.S. Strategic Command, for performing operational planning and execution of offensive and defensive cyberspace operations.

These responsibilities, unified under a single commander, are the cornerstone of 16th Air Force's ability to converge on problems and generate outcomes on strategic competition. It is the integration of the various operational capabilities and access to global data, leveraged against specific problems, with the appropriate organic authorities, and acting by, with and through partners, that forms the foundation of information warfare.

Source: https://www.16af.af.mil/.

## E. Coast Guard Cyber Command

**Mission**.

- **Defend Coast Guard Cyberspace**: Operate and maneuver the Coast Guard Enterprise Mission Platform to assure Coast Guard mission execution in all domains, while aggressively defending our part of the DOD Information Network (DODIN).
- **Enable Coast Guard Operations**: Enable Coast Guard operations at sea, in the air, on land and space by delivering effects in and through cyberspace.
- **Protect Maritime Transportation System (MTS)**: Protect maritime critical infrastructure by delivering effects and capabilities in and through cyberspace.

**Vision**. Ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure.

**Lines of Effort**. U.S. Coast Guard actions are organized into three lines of effort: (1) Defend and Operate the Enterprise Mission Platform; (2) Protect the Marine Transportation System; and (3) Operate In and Through Cyberspace. These efforts will be underpinned by development and sustainment of a skilled workforce, intelligence driven operations, and domestic and international partnerships to achieve unity of effort.

**CGCYBER Departments**.

- **Cyber Intelligence (CGCC-2)**. The CGCYBER Intelligence Department, CGCC-2, provides intelligence support internally to the CGCYBER Operations Department (CGCC-3), CGCYBER / Deputy CGCYBER, and Planning and Policy Department (CGCC-5). CGCC-2 also collaborates with Coast Guard Intelligence components, Intelligence Community (IC) components, and to leadership within Department of Homeland Security (DHS), Department of Defense (DOD), and Coast Guard, as requested.
- **Operations Department (CGCC-3)**. CG CYBER Operations Department consists of CGCC-33 Network Operations and Security Center, and CGCC-35 Future Operations Division. CGCC-3 is also the parent command of the Cyber Protection Team, the Cybersecurity Operations Center, and the Maritime Cyber Readiness Branch. Mission elements of CGCC-3 include the Cyber Protection Team (CPT), the Cybersecurity Operations Center (CSOC), and the Maritime Cyber Readiness Branch (MCRB). The CPT is the Coast Guard's deployable unit responsible for offering cybersecurity services to the Marine Transportation System (MTS). MCRB is a component of CGCYBER that focuses on cybersecurity in the commercial maritime transportation community.
- **Assessment and Authorization (CGCC-AA)**. CGCC-AA is responsible for establishing processes for all A&A functions in order to standardize how the Coast Guard conducts assessments and authorizations for Coast Guard (CG) Information Technology (IT).
- **Operations Support**. The CGCYBER Operations Support Department provides Administrative, Budget / Resources, Security, and Training & Exercises support.

Sources: https://www.dco.uscg.mil/Our-Organization/CGCYBER/ and https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG_Cyber_Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3d%3d.

**Intentionally Blank**

# Glossary

Terms are taken from the *DOD Dictionary of Military and Associated Terms* (as of May 2022) and the Cybersecurity and Infrastructure Security Agency (CISA) 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 operations (EMSO)** — Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment.

**electromagnetic spectrum superiority** — That degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same.

**electromagnetic 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).

Intentionally Blank



CENTER for STRATEGIC LEADERSHIP

CSL