PERSPECTIVES ON CYBER POWER

CPP-9

AIR FORCE CYBER LAW PRIMER

Lt Col Royal A. Davis III, ACC/JA, Director
Jeffrey T. Biller, USAFA, Editor in Chief
and Cyber Law Primer Team

AIR FORCE CYBERWORX
AIR FORCE ACADEMY
LAW, TECHNOLOGY, AND WARFARE RESEARCH CELL

AIR UNIVERSITY

AIR UNIVERSITY PRESS

Air Force Cyber Law Primer

Lt Col Royal A. Davis III, ACC/JA, Director
Jeffrey T. Biller, USAFA, Editor in Chief
and
Air Force Cyber Primer Team

CPP-9

Air University Press
Maxwell Air Force Base, Alabama

Director, Air University Press
Dr. Paul Hoffman

Project Editor
Jeanne K. Shamburger

Illustrator
Catherine Smith

Print Specialist
Nedra Looney

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Accepted by Air University Press May 2021 and published November 2022

ISSN 2831-5251

Cover photo: National Security Operations Center floor, NSA headquarters, in 2012. National Security Agency photo.

Perspectives on Cyber Power

We live in a world where global efforts to provide access to cyber resources and the battles for control of cyberspace are intensifying. In this series, leading international experts explore key topics on cyber disputes and collaboration. Written by practitioners and renowned scholars who are leaders in their fields, the publications provide original and accessible overviews of subjects about cyber power, conflict, and cooperation.

As a venue for dialogue and study about cyber power and its relationship to national security, military operations, economic policy, and other strategic issues, this series aims to provide essential reading for senior military leaders, professional military education students, and interagency, academic, and private-sector partners. These intellectually rigorous studies draw on a range of contemporary examples and contextualize their subjects within the broader defense and diplomacy landscapes.

These and other Cyber Papers are available via the AU Press website at https://www.airuniversity.af.edu/AUPress/.

Air Force Cyber Law Primer Team Members

Lt Col Royal A. Davis III, ACC/JA, Director/Author
Prof. Jeffrey T. Biller, USAFA, Editor in Chief/Author
Ms. Rebecca K. Lively, 16 AF/JA, Editor/Author
Maj Vincent L. DeFabo, 67 CW/JA, Editor/Author
Mr. Rafael A. Martinez, ACC/JA, Editor/Author
Mr. Eric G. Rosenberg, 67 CW/JA, Author/Reviewer
Maj Thomas R. Burks, 16 AF/JA, Author
Maj Dimple N. Chheda, NGB/JA, Author
Maj Patrick A. Clary, HQ USCYBERCOM/JA, Author
Maj Jasmine A. Dixon-Sims, 16 AF/JA, Author
Capt Christopher J. Elliott, 16 AF/JA, Author
Maj William D. Toronto, HAF/JA, Author
Maj Gordon H. Hage, USAFR, Author
Maj Alexandra K. Holtsclaw, 67 CW/JA, Author
Maj Aaron D. Kirk, 67 CW/JA, Author
Maj Jonathan K. Sawmiller, 16 AF/JA, Author
Maj Trenton M. White, 16 AF/JA, Author
Lt Col Vicki A. Belleau, HAF/JA, Reviewer
Sqn Ldr Daniella S. Biedla, RAF Exchange Officer, Reviewer
SQNLDR Anthony Erman, RAAF Exchange Officer, Reviewer
Mr. Liam R. Harrell, 67 CW/JA, Reviewer
Ms. Emma K. McAllister, ACC/JA, Reviewer
Maj Kelby D. Kershner, ACC/JA, Contributor

Contents

List of Illustrations

Figures

Tables

Foreword

Cyber law is a broad discipline that is constantly evolving and growing as technology and applicable law continue to develop. The terminology is highly technical, often colloquial, and occasionally less than clearly defined. Your clients will know the lexicon contained herein fluently. However, they will not always be able to draw forward the legal relevance of the same. Consequently, attorneys and paralegals must inform themselves on the technical aspects of cyber operations to properly advise clients and identify legal issues—many of which will be without precedent. This project was comprised entirely of volunteers and culminates hundreds of hours of time—a considerable portion of which was personal off-duty time. This primer seeks to expedite the rigorous process of learning the practice of cyber law.

Chapter 1

Cyberspace Overview

I. Introduction

A. The Internet. The Committee on National Security Systems (CNSS) defines the *Internet* as "the single interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Name, and Numbers (ICANN).[1]

1. The Internet provides a standardized means for end-to-end networking across multiple global networks, often of disparate organizational origin and physical characterization. However, what makes the Internet work effectively are common upper levels of network-hosted Internet Protocol (IP) "stacks."
2. The CNSS defines a *host* as "any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. An *IP* is defined as the "standard protocol for transmission of data from source to destination in packet-switched communications networks and interconnected systems of such networks."

B. The CNSS. Formerly the National Security Telecommunications and Information Security Committee (NSTISSC), the CNSS was rebranded by Executive Order 13231.[2] The CNSS is an intergovernmental agency tasked with setting national-level information assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government (USG) departments and agencies for the security of national security systems (NSS) through the CNSS issuance system. When performing research, it is essential to remember that directives predating 2001 will still be referenced by their NSTISSC label but remain authoritative documents until rescinded.

II. Technology

A. Protocols and Software

1. Transmission Control Protocol / Internet Protocol (TCP/IP). The Internet uses the TCP/IP protocol to send and receive information. Sending an entire file in one transmission would require a sus-

tained connection between the sending and receiving devices. It presents many potential reliability problems, such as connection interruptions before the transfer is complete, requiring the whole transfer to begin again. TCP/IP allows the file to be sent in smaller chunks, enables multiple paths to find the most efficient route for each chunk, and requires only missing or corrupted pieces to be resent. The sending device uses TCP to break the data into packets and tracks which packets have been sent and received. Each packet has a heade, with information lik, the IP address and the packet sequence number.

2. IP "protocol" uses the IP address to send the packets through routers to the destination. Routers are devices that maintain tables of IP addresses and direct network traffic to the most efficient route for each packet. Each router a packet travels through is called a *hop*. The packets can take several different paths from the sender to the receiver. The receiving device sends back an acknowledgment so the sending device can verify all packets were received and resend missing packets if needed. The receiving device uses TCP to reassemble the packets into the original data. For example, a file sent from a home computer in Texas to a home computer in New York travels from the computer to the home router, to a router at the Internet service provider (ISP), through the most efficient path for each packet until it reaches the receiver's ISP in New York, to the receiver's home router, and finally to the receiver's computer where it is reassembled into the original file (fig. 1.1).

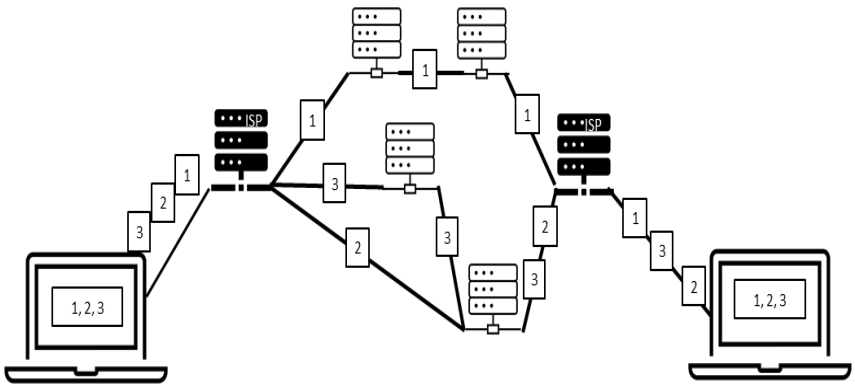


Figure 1.1. Network transmission

3. Dynamic Host Configuration Protocol (DHCP) Servers. A DHCP server constantly listens for new devices and, once heard, assigns an IP address to those computers or other devices. The system administrator runs DHCP servers from an ISP or the installation. DHCP servers also send information to routers. A DHCP server tells a device its address and the next network segment the data packet will travel or hop. IP addresses are currently 32 bits (binary digits) of information separated into four separate numbers ranging from 0 to 255 (e.g., 12.244.16.255). Using 32-bit IP addresses allows for up to approximately 4 billion IP addresses worldwide. An individual router does not need to maintain a table with a complete list of every IP address. It can match the prefix and direct the packet closer and closer to the destination until it reaches a router with the exact destination IP address in its table. The current IP version is called IP Version 4 (IPV4). However, with the advent of the Internet of Things (IoT), there are, or soon will be, insufficient IP addresses under IPV4 to adequately assign addresses to the number of devices in use. Consequently, private and public organizations have begun implementing IPV6, a 128-bit system that allows 340 undecillion (34 with 37 places after it) possible IP addresses.

4. Malware. Also referred to as malicious code or malicious logic, the National Institute of Standards and Technology (NIST) defines *malware* as "software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code."[3]

5. Cloud. The NIST defines *cloud computing* as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources," such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort.[4]

    a) In broad terms, cloud computing is the practice of remotely storing and accessing information and software on demand rather than storing the software on a system's drive or through some other organizational intranet server. The NIST has identified four cloud computing models: public, private, community, and hybrid. These models vary with where the hardware is

located, what entity is responsible for maintaining the system, and who can use system resources. For legal practitioners, the central issue is what type of cloud, if any, your installation uses, keeping in mind that there may be several.

b) The U.S. Federal Cloud Computing Strategy outlines the USG's intent to move from the legacy "Cloud First" (unsuccessful cloud initiative) to "Cloud Smart" and contains several overarching statements regarding the USG's approach to cloud computing.[5] The Department of Defense (DOD) issued a Software Modernization Strategy in February 2022 that "provides the approach for achieving faster delivery of software capabilities in support of Department priorities such as Joint All Domain Command and Control and artificial intelligence."[6] Both documents provide insight into how the DOD intends to migrate to a cloud-based architecture.

c) In the DOD, the main initiative to modernize cloud computing architecture is the Joint Warfighter Cloud Capability (JWCC). This program is the successor to an earlier initiative known as the Joint Enterprise Defense Infrastructure (JEDI) program, a $10 billion, 10-year firm-fixed-price (FFP) contract. The indefinite delivery/indefinite quantity (ID/IQ) contract was initially awarded to Microsoft. Amazon Web Services (AWS) successfully challenged the award, and the JEDI program was subsequently scrapped. The JWCC contract is due to be awarded in December 2022 and will likely be the service provider that many DOD installations will use for cloud computing and storage services.

d) In the interim, many commanders will be interested in pursuing alternatives to the overarching general purpose JWCC architecture under a pathfinder or other programmatic construct. Local procurement at the installation level will likely need to go through a program of record. For example, the Defense Information Systems Agency (DISA) operates a "private cloud" called milCloud, while an example of a "community cloud" authorized for USG use is Amazon's GovCloud. Any procurement under these architectures must be thoroughly vetted through your communications squadron and contracting squadron professionals. Additionally, all commercial cloud procurements

must undergo relevant acquisition processes. Procurement guidance updates for commercial cloud initiatives are available at https://www.esi.mil/.

e) Additional Cloud-Specific Training Resources:

(1) Defense Acquisition University, *DoD Cloud Computing Acquisition Guidebook* (comprehensive): https://www.dau.edu/

(2) AWS Cloud Training: https://aws.amazon.com/training/

(3) Oracle Cloud Training: https://education.oracle.com/

6. Artificial Intelligence (AI). Neither NIST nor CNSS has promulgated an official definition of *AI* at the time of this writing. The 2018 DOD AI Strategy states that "AI refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems."[7] The 2021 National Defense Authorization Act (NDAA), Section 501, defines *artificial intelligence* as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. In March 2019, the Air Force promulgated an annex to the same.[8] On June 27, 2018, the Secretary of Defense (SecDef) established the Joint Artificial Intelligence Center (JAIC).[9] In February 2020, the SecDef published the Artificial Intelligence Ethical Principles for the Department of Defense. The five DOD AI ethical principles for design, development, deployment, and use of AI capabilities are responsible, equitable, traceable, reliable, and governable. The DOD chief information officer (CIO), through the JAIC, serves as the DOD's lead for coordination of oversight and implementation of the principles. In March 2021, the National Security Committee on Artificial Intelligence released its "Final Report." It comprises 16 chapters explaining the steps the United States must take to responsibly use AI for national security and defense, defend against AI threats, and promote AI innovation.[10] The critical takeaway for practitioners is that AI development is in the early stages. Capabilities development contracts for the foreseeable future will likely remain centrally managed either through the JAIC, NIST, or Service-specific laboratories (e.g., Air Force Research Laboratory).

7. Remote Access Tools. The NIST defines *remote access* as "access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet)."[11] A remote access tool (RAT) is specialized software or a combination of software and hardware that allows a user to gain "remote access" to an information system. In operational contexts, this may entail unauthorized remote access to an adversary's information system.

B. Additional Technology Training Resources

1. Free online training addressing these and more advanced topics is available to all federal employees, including Service members, at https://fedvte.usalearning.gov/. Courses include Cyber Fundamentals for Law Enforcement Investigations and Emerging Cyber Security Threats.
2. MITRE runs the open-source web page ATT&CK where experts discuss and track multiple cybersecurity and observed attack methods, tactics, techniques, and procedures (TTP): https://attack.mitre.org/.
3. The DOD Cyber Crime Center (DC3) Cyber Training Academy also provides online webcasts and courses on a wide range of technology and cybersecurity topics at https://www.dcita.edu/. A DOD Common Access Card (CAC) is required to register.

III. DOD's Doctrinal Approach to Cyberspace

A. The DOD defines *cyberspace* as 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."[12] The President, SecDef, and Chairman of the Joint Chiefs of Staff (CJCS) have all promulgated strategic guidance with impacts on cyberspace operations (CO).[13]

B. The DOD conceptually divides cyberspace into three layers: (1) a physical network layer, (2) a logical network layer, and (3) a cyber-persona layer. The physical network comprises the geographic and physical network components. The logical network comprises related elements abstracted from the physical network (e.g., a website hosted on servers in multiple locations but accessed through a single URL).

The cyber-persona layer uses the logical network layer rules to develop a digital representation of an individual or entity identity.

1. From a legal perspective, distinguishing between these layers is important. At the physical layer, website data may be stored entirely in one country. The logical layer may utilize networks in multiple countries to send the data to a particular user. In contrast, the cyber-persona layer may be directed at, and primarily accessed from, persons residing in a country other than where the data is stored. This scenario raises challenging jurisdictional and choice-of-law questions for any legal practitioner.

2. More specifically, think about hate speech laws and how the three layers of cyberspace complicate the legal analysis facing a prosecutor or policy maker. Imagine a U.S.-based publication using a commercial service in Canada to manage its online content while the Canadian company uses servers in Ireland. Some content is intentionally directed at a German audience, which has ready access to the online publication via its publicly available URL. German prosecutors determine the website's content violates German restrictions on hate speech and want to enjoin the publication. Who has jurisdiction, and whose law should govern?

3. From the physical layer perspective, the content is stored on a server in Ireland, which has no genuine interest in the harm felt against German or U.S.-specific speech rights. The publisher and its agent are in the U.S. and Canada, respectively, both having a strong interest in protecting businesses and their nation's speech laws. At the logical layer, the content continually transits foreign networks and is available anywhere there is access to the URL. At the cyber-persona layer, some of the content was directed primarily, but not exclusively, at German-language speakers.

4. Invariably, Germany maintains an interest in enforcing its speech laws, even if the content originated outside the country. However, the U.S. has a strong interest in protecting the American speaker who generated the online content. Canada wants to maintain its business interest in hosting online content and protect its speech standards. Should the law require the U.S company to modify its content to comply with all nations' laws, no matter how sensitive and inconsistent with U.S. values? Or should U.S.-based publications be required to comply only with U.S. speech laws—in essence,

imposing U.S. standards on all locations with Internet access and frustrating local sensibilities? In sum, reaching an answer on these questions is a complex process requiring consideration of many competing variables.

5. Take another hypothetical scenario aligned to military cyberspace operations. Imagine an international terrorist organization seeking to harm U.S. troops in the U.S. Central Command (CENTCOM) area of responsibility (AOR). This group uses commercially available cyber infrastructure in Zimbabwe to store and disseminate its propaganda, recruit new members, and solicit funding and other types of support. The U.S or its allies may seek to interrupt the terrorist's online operations. The server is in Zimbabwe, which exercises sovereignty authority over the server and its associated cyber infrastructure from a physical layer perspective.[14] From a logical layer perspective, anyone with an Internet connection can access the server and its information. From a cyber-persona perspective, the information is targeted at individuals sympathetic toward the terrorist organization's cause and who would like to see harm to the U.S. and its allies. Thus, the ultimate effects are most likely to be felt in the CENTCOM AOR by U.S. and allied units. Whose interests should predominate in this circumstance? Those of Zimbabwe? The countries most likely to be targets of the terrorist group's operations? Again, there are many variables to consider.

6. In sum, advising on cyber law requires an understanding of cyberspace's three layers—physical, logical, and cyber-persona—which must be distinguished and incorporated into legal advice. Each layer reflects the distinct nature of cyberspace and the many jurisdictional challenges that arise in this practice.

C. The DOD further conceptualizes cyberspace as constituting three major maneuver areas. Joint Publication (JP) 3-12, *Cyberspace Operations*, classifies these areas as "blue, "gray," and "red" cyberspace. The three maneuver areas have operational, and often legal, importance given that they roughly define the areas of cyberspace we can access, versus areas either owned or controlled by third parties or adversaries. There is no such term as "stateless maneuver space" in cyberspace—that is, maneuver in cyberspace often transits multiple sovereign nations irrespective of the purpose. Legal practitioners must be aware of the system from which a given operation may originate, what area of

cyberspace the operation is transiting through, and where the final effect of that cyber operation is intended to occur. JP 3-12 defines the following tricolor framework for classifying cyberspace.

1. Blue Cyberspace. *Blue cyberspace* denotes areas protected by the U.S. Government and its mission partners and other areas where the DOD may be ordered to protect or has consent to operate. The DOD has standing orders to protect the Department of Defense Information Network (DODIN).

    a) The DOD may, when requested by other authorities and approved consistent with law and policy, defend or secure other areas of cyberspace, particularly within the U.S. Government. Additionally, the Department of Homeland Security or foreign nations may request that the DOD defend cyberspace related to critical infrastructure and key resources (CI/KR) of both the U.S. and partner nations. Maneuvering in blue cyberspace includes positioning forces, sensors, and defenses to secure the area or engage in defensive actions.

    b) From a legal perspective, blue cyberspace refers to domains and networks for which we have authorized legal access and are operating within the scope of that authorization. Gray cyberspace can become blue cyberspace with the network owner's consent and appropriate U.S. Government agency authorization. The DOD cannot guarantee the robustness of the security standards applied to non-DOD networks and systems. Thus, the commander's mission risk analysis should account for this uncertainty in non-DOD cyberspace security. Examples of blue cyberspace include your DOD workstation, weapon systems such as the computer systems on an F-16 and its associated cyber platforms, and any DOD-issued smartphone. Also included are systems, switches, and routers the U.S. Government is authorized to access (i.e., through a lease) or otherwise owns or controls.

2. Red Cyberspace. *Red cyberspace* refers to areas owned or controlled by an adversary or enemy. In this instance, "controlled" means more than "having a presence on," as adversaries may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact on system operation. Here, "controlled" means the ability to direct the operations of a link, node, or enclave of cyberspace to the exclusion of

others. Examples include workstations, cell phones, servers, routers, networks, or network enclaves controlled by an adversary.

3. Gray Cyberspace. *Gray cyberspace* is that which fails to meet the description of either "blue" or "red" cyberspace. Gray cyberspace (off-DODIN operations) may be necessary to gain access to intermediary links and nodes in support of future operations. Examples include your personal cell phone or tablet, a coffee shop's free Wi-Fi network, corporate servers or networks, and telecommunication companies in countries not targeted by a specific operation. Most civilian servers and networks are considered gray cyberspace.

D. The DOD Information Network. United States Cyber Command (USCYBERCOM) has the Presidentially assigned mission to direct operations in defense of the DODIN. JP 3-12 defines the *DOD Information Network* as the "end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters . . . whether interconnected or stand-alone." The Air Force Information Network (AFIN) is a portion of the DODIN.

1. AFIN. Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*, defines the *Air Force Information Network* as "the set of Air Force 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." It includes the Air Force Network (AFNET), Air Force Network—Secure (AFNET-S) enterprise networks, and many other networks.[15]

2. Air Force Instruction (AFI) 17-201, *Command and Control (C2) for Cyberspace Operations*, defines the *Air Force Network* as "the Air Force's underlying Nonsecure Internet Protocol Router Network [NIPRNet] that enables Air Force operational capabilities and lines of business, consisting of physical medium and data transport services." It defines the *Air Force Network—Secure* (AFNET-S) as the "Air Force's underlying Secure Internet Protocol Router Network (SIPRNet) that enables Air Force operational capabilities and lines of business, consisting of physical medium and data transport

services. AFI 17-201 adds that the AFNET "includes transmission mediums, gateways, routers, switches, hubs and firewalls, and the functions required to support and enable the environment," including C2, network authentication, and defense.[16]

3. Many use the terms *AFIN* and *AFNET* interchangeably. However, they do not mean the same thing. The Air Force Information Network is the broader term that defines owned and leased Air Force networks and the information and applications contained thereon. Conversely, the Air Force Network focuses on the physical Air Force network infrastructure.

4. Domain. The term *domain* or *security domain* means an environment that "implements a security policy and is administered by a single authority."[17] A hierarchy organizes all domain names. Domain names such as .gov or .mil are called "sponsored top-level domains" (TLD). The Department of Commerce administers all TLDs in the United States under the Secure Domain Name System (DNS).[18] The sponsor for the .mil TLD is DISA. Names going to the left of the .gov, .mil, or .us domains are second-level or "enterprise" domains. A sponsored TLD may also be referred to as an "enclave" in practice. Practitioners need to understand that each domain worldwide has a unique identifier and a separate security system associated with it. For example, if you are on the afcent.mil domain, there will be two separate security owners for each domain or enclave.[19]

IV. The Network

A. Access to the Network. Access to the DODIN and subordinate departmental networks is governed primarily by DISA, designated a combat support agency under the Goldwater-Nichols Act.[20] DISA "plans, engineers, acquires, tests, fields, operates, and assures information-sharing capabilities, command and control (C2) solutions, and a global enterprise infrastructure to support DoD and national-level leadership."[21]

1. A process referred to as "transport" or "transit" governs access to networks and network data. As noted above, the DODIN consists of all networks and information systems owned or leased by the DOD. The DODIN includes all classified and unclassified common enterprise service networks (e.g., SIPRNet, Joint Worldwide Intelligence

Communications System [JWICS]), intelligence networks operated by DOD components within the intelligence community (IC) (e.g., National Security Agency Network [NSANet]), closed-mission systems and battlefield networks, and other special-purpose enclaves (e.g., research and development and combatant command networks like afcent.mil).[22]

a) The AFIN is a DOD component enclave infrastructure that relays data through a more extensive global system, managed and configured by DISA, called the Defense Information Systems Network (DISN). The DISN is a DOD-owned and DOD-leased telecommunications and computing systems integrated network grid. The DOD CIO controls access to the DISN, who has delegated that authority to the DISA director. The CIO is tasked with overseeing, managing, and advising on the entire enterprise information technology architecture under 40 U.S.C. §11315. Access to the separate DOD component enclaves, such as the AFIN and AFNET, are governed through the service CIOs. At the time of this writing, the Air Force CIO is Ms. Lauren Knausenberger, SAF/CN. The CIO process governs access to any DOD network.[23]

b) The CIO or their designee (typically the MAJCOM/A6) grants access to any Air Force–controlled (i.e., owned/leased) network through the DISA-operated Enterprise Mission Assurance Support Service (eMASS) system.[24] Any entity seeking to connect a device to the network must submit a request through this process and explain items such as endpoint security protocols for the device (i.e., McAfee virus scan), data-loss prevention, and intrusion detection systems that the device will use.

c) The application must also identify the enclave the device will connect from and describe the boundary and access point where the device will enter the network. The below graphic demonstrates an application seeking access to the AFNET and the gateways from which the system and device will operate.[25] For systems and enclaves connecting to and through the AFNET or AFNET-S, Approval to Connect (ATC) requests are submitted to the Air Force Enterprise authorizing official (AO) through the "Manage ATC" function in eMASS. Contact the Air Force Enterprise AO staff for additional connection (contractor, commercial Internet service provider, direct) information and guid-

ance. From a legal perspective, understanding the system boundary (i.e., AFNET versus AFIN) may drive vastly differing analyses, particularly in cases where the Air Force leases or owns the system or device.

d) Only approved devices may connect to the DODIN. DISA posts a running searchable Approved Products List (APL) to its website at https://aplits.disa.mil/processAPList.action, or you or your client may also send specific questions to their org box at disa.meade.ie.list.approved-products-certification-office@mail.mil.

2. Network Boundary. The Office of Management and Budget (OMB) defines a *boundary* as "all components of an information system to be authorized for operation by an authorization official . . . [and] excludes separately authorized systems to which the information system is connected."[26] The OMB creates policy here due to its overarching acquisition authority under 40 U.S.C. §11314. OMB Circular A-130 outlines how authorizing officials may grant access to their specific network boundary. It is important for legal professionals to note that a boundary may be an authorization boundary for a system, the organizational network boundary, or a logical boundary defined by the organization.[27]

a) This guide has previously covered the definitions of the DODIN, the AFIN, and the AFNET to describe the physical and logical networks used and protected by various cyber operators. We have also discussed the broader concepts of blue, gray, and red cyberspace. For judge advocates practicing cyber law, understanding the applicable operational authorities and limitations is critical. Thus, it is worth considering what "bounds" these networks and how information travels between them.

b) Air Force installations are typically set up as "base enclaves" where the Air Force typically owns the underlying network. These enclaves have internal/external routers controlling traffic in and out of the enclave and a firewall providing the base's secure boundary. Some installations use multiple routers for this purpose. Department of the Air Force (DAF) traffic between bases is normally routed differently than traffic intended for the commercial Internet. If directed toward another DAF base, the traffic skips the Air Force Gateway and travels directly between

bases on the AFNET over network lines leased from, or controlled by, DISA.

c) The AFNET connects to the commercial Internet through suites of equipment known as gateways. Any network traffic traveling between Air Force systems and the Internet is required to pass through these gateways. The gateways consist of unclassified and classified external service delivery points, a security boundary, and an Air Force Intranet service delivery point with multiple security levels at the gateway components. Integrated management sites located at the 26th Network Operations Squadron (Gunter AFB, Alabama) and the 33rd Network Warfare Squadron (Lackland AFB, Texas) manage these gateways. These gateways connect to the Internet by using DISA's long-haul connections framework (NIPRNet and SIPRNet). The gateways were in the process of being replaced under DISA's Joint Regional Security Stack (JRSS) program. However, in 2021 the DOD made the decision to sunset the JRSS program in favor of a future zero-trust solution. The JRSSs are suites of equipment, typically 20 racks in each, that manage and defend traffic flows while also providing DOD big data analytics functionality. The services provided by the JRSS include transport and cyber security functions, including logical separation of traffic, independent virtual firewalls, intrusion detection and prevention, and enterprise management.

   (1) The distinction of where the AFNET ends and the commercial Internet begins is critical to understand for attorneys advising on cyberspace operations and security. This boundary could trigger different legal authorities and marks the physical and logical separations between blue and gray cyberspace analytical constructs. Notably, DISA's long-haul communications network services are provided to the Air Force contractually. While not part of the AFNET, these communication networks still constitute blue space.

   (2) The implementation of the JRSS program is ongoing in the Air Force. Currently, the Air Force still uses boundary intrusion prevention systems (BIPS), host intrusion prevention systems (HIPS), firewalls, network traffic security analyzers (NTSA), and Web proxies as part of the gateway architecture to provide security for the AFNET.

(3) SIPR traffic tunnels through the NIPR networks using cryptological protections to route separately from NIPR traffic. In many ways, SIPR functions in the same manner as a virtual private network (VPN).

(4) The Joint Worldwide Intelligence Communications System (JWICS) traffic runs across separate networks owned by the Defense Intelligence Agency (DIA).

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Committee on National Security Systems Instruction (CNSSI) No. 4009, *Committee on National Security Systems (CNSS) Glossary*.
2. Executive Order No. 13231, Critical Infrastructure Protection in the Information Age.
3. U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, 407.
4. U.S. Department of Commerce, NIST SP 800-145, *NIST Definition of Cloud Computing*.
5. Kent, *Federal Cloud Computing Strategy*.
6. Department of Defense, *Department of Defense Software Modernization Strategy*.
7. Department of Defense, *Summary of the 2018 Artificial Intelligence Strategy*.
8. Department of the Air Force, *United States Air Force Artificial Intelligence Annex*.
9. Deputy Secretary of Defense to chief management officer of the Department of Defense et al., memorandum.
10. See the National Security Commission on Artificial Intelligence at https://www.nscai.gov/.
11. U.S. Department of Commerce, NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*.
12. Joint Publication (JP) 3-12, *Cyberspace Operations*, GL-4.
13. See JP 3-12, table 1.3.A.
14. Sovereignty is discussed in more depth in chap. 2.
15. Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*.
16. AFI 17-201, *Command and Control (C2) for Cyberspace Operations*.
17. U.S. Department of Commerce, NIST SP 800-53, rev. 5, *Security and Privacy Controls*.
18. U.S. Department of Commerce, NIST SP 800-81-2, *Secure Domain Name System (DNS) Deployment Guide*.
19. Department of Defense Instruction (DODI) 8410.01, *Internet Domain Name and Internet Protocol Address*.

20. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. 99-433, 100 Stat. 992.

21. DOD Directive 5105.19, *Defense Information Systems Agency (DISA)*.

22. DODI 8010.01, *Department of Defense Information Network (DODIN) Transport*.

23. For the connection process to the AFIN, see AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, para. 6. For enclaves requiring a circuit connection from the Defense Information Systems Agency, information systems security managers must follow the Defense Information System Network Connection Process Guide to ensure all required artifacts are provided on initial submission. Connection requests will be coordinated through the AF Enterprise authorizing official (AO). For connection to the Air Force Information Networks, the Air Force Enterprise AO is the only authority permitted to grant an Approval to Connect (ATC) to the AFIN. ATC authorities for other AF appointed AOs may be approved by SAF/CN in coordination with the Enterprise AO.

24. Given the developing command structure of the United States Space Force, equivalent Space Force units are not included in this version of the primer. Future versions will include equivalent Space Force units.

25. For additional information, see DISA, "eMASS," fact sheet.

26. OMB Circular No. A-130, Subject: Managing Information as a Strategic Resource.

27. U.S. Department of Commerce, NIST SP 800-53, rev. 5, *Security and Privacy Controls.*

Chapter 2

International Legal Considerations

I. Introduction

All operations, including cyberspace operations, must analyze three basic sets of authority: first, international legal considerations; second, domestic law authorities and limitations; and third, domestic policy requirements. This chapter addresses the first category. International law applicable to military operations is a broad and quite complex field of study. This section is not exhaustive, as it is intended as a primer alone. Certain subjects, such as the law of neutrality, are omitted not due to their lack of importance but to focus on foundational issues. More detailed studies on the application of international law to cyberspace operations can be found in many places, such as the following. However, legal practitioners should be highly aware of the standing and value of each study.

A. *Law of War Manual*. In the U.S., the DOD *Law of War Manual* (*LOWM*) provides practitioners and operators with official DOD policy regarding international law as it applies to military operations.[1] The DOD *LOWM* covers DOD policy and guidance in the *jus ad bellum* and *jus in bello* frameworks. Chapter 16 of the *LOWM* covers cyber operations specifically. Practitioners should be aware that the DOD *LOWM* is not always explicit about the distinction between the U.S. understanding of formal international law and policy guidance based on national security objectives. Therefore, practitioners should also look to primary sources such as treaty law and formal U.S. statements on *opinio juris*.

B. *Tallinn Manual 2.0*. The DOD General Counsel, in his remarks at the United States Cyber Command (USCYBERCOM) Legal Conference on March 2, 2020, stated that initiatives by nongovernmental groups like those that led to the *Tallinn Manual* can be useful to consider but do not create new international law, which only States can make. The *Tallinn Manual* is an extensive study and compilation of how international law applies to cyber operations. It was compiled by an international group of experts (IGE), international scholars, and experts in the field. It also received reviews and feedback from several State representatives, although it does not wholly represent any State's for-

mal opinion.[2] The *Tallinn Manual* is an excellent research source that can help a practitioner spot issues and understand some of the debates around key tenets of international law. However, it should be referenced with caution when it comes to practical advice to commanders, as it conflicts—or at least goes beyond—the U.S. formal position on several issues. It must be reemphasized that the manual does not represent official DOD, U.S., or NATO policy and is not international law. USCYBERCOM's official position on the manual is that it is a good place to start a conversation but should not be adhered to as policy or guidance.[3]

C. Sources of International Law. Article 38 of the International Court of Justice (ICJ) treaty provides one broadly accepted definition of sources of international law. According to Article 38, the following are sources of international law, ranked in order of precedence: treaties establishing rules recognized by States party to the treaty, customary international law, general principles of law, and judicial decisions and the teachings of the most highly qualified publicists as a subsidiary means for the determination of rules of law. We focus here primarily on the first two categories.

II. Customary International Law

A. Although no treaties govern cyber operations specifically, a significant body of rules based on general international law guides cyber operations both in peacetime and armed conflicts. International law takes the form of either customary international law (CIL) binding on all States or treaty law for States party to a particular treaty. States are prohibited from conducting cyber operations that constitute an internationally wrongful act, which has two elements. The first element is a breach of an international legal obligation. Illegal uses of force and violations of the rule of distinction within an armed conflict are two examples of a breach and are discussed below. The second element is an action attributable to a State. Legal obligations come from treaty and customary international law. Legal attribution is a product of CIL. We first turn to its formation and development.

B. Customary International Law Development

1. CIL emerges over time through a combination of State practice and *opinio juris*—short for the phrase *opinio juris sive necessitatis*, meaning "an opinion of law or necessity." That is, *opinio juris* is

evidence of a State's belief that a given practice is mandatory. A critical characteristic of CIL is that it is "an unwritten form of law in the sense that it is not created through a written agreement by States."[4] CIL may constitute rules with no representation in treaty law, such as the principle of non-intervention. It may also serve to interpret existing treaty law in unclear circumstances, such as rules governing cyber operations under the law of war (LoW).

2. Whether a rule or norm of behavior has become customary international law is not always clear. Ideally, organizations such as the Department of State Office of the Legal Advisor or the DOD Office of General Counsel (OGC) will have made explicit statements of *opinio juris* that legal practitioners can apply in the field. Generally, declarations by a government representative with authority to make such a representation of that State's understanding of international law, and its corresponding obligations, may be considered evidence of *opinio juris*.[5] However, the practitioner must also be wary of remarks not intended to constitute *opinio juris*, such as heated rhetoric immediately following an international incident.

3. An excellent example of a formal statement of *opinio juris* regarding cyber operations came in March 2020, when the Honorable Paul C. Ney Jr., General Counsel of the DOD, relayed the DOD's position on international and domestic law during a USCYBERCOM-hosted legal conference. References to his speech, as well as other sources of CIL, are included throughout this primer.

C. Principle of Non-intervention

1. As mentioned, formal legal obligations sometimes stem from CIL. Particularly relevant to cyber operations is the principle of non-intervention. This rule of CIL prohibits States from intervening, by coercive or dictatorial means, in another State's *domaine réservé*. The *domaine resérvé* constitutes matters that each State is permitted, by the principle of State sovereignty, to decide freely, such as political, cultural, and economic systems.[6] Interference in elections through cyber operations is a recent example of the debate over the application of non-intervention in the cyber domain.[7]

2. While a violation of the non-intervention principle does not permit a response with force, it does justify countermeasures, which are themselves customary. Countermeasures are State responses to

unlawful operations of another State that would likewise be unlawful if not for the offending State's conduct. Only victim States may employ countermeasures and only in an attempt to bring the offending State back into compliance with international law. Additionally, countermeasures cannot rise to the level of a use of force, which may make cyber operations a particularly effective tool for countermeasures.[8]

D. Sovereignty

1. The principle of non-intervention is an accepted rule of international law, although application to individuals' fact patterns can be quite contentious. A rule of sovereignty, on the other hand, is a controversial topic. The existence of a principle of sovereignty that undergirds many rules of international law is well accepted. For example, the rules of territorial seas and airspace are manifestations of this principle. However, many of these rules find their sources in treaty law, such as the United Nations (UN) Convention on the Law of the Sea.[9] Others, such as the above principle of non-intervention, are considered CIL.

2. There is a current and unresolved debate about whether there is a standalone CIL rule of sovereignty that would apply in cyberspace and govern malicious cyber operations that do not implicate the UN Charter or constitute a prohibited intervention. Again, the United States has taken no formal position on this issue. However, legal practitioners should be aware of the debate and understand the potential implication of all positions.[10]

E. Legal Attribution

1. States frequently use groups or individuals that do not formally belong to a State to conduct malicious cyber operations. This tactic's use is primarily due to the requirement for any action to be attributable to a State to satisfy an internationally wrongful act's legal requirements. Legal attribution is also referred to as a State responsibility and finds its most substantial reflection in the International Law Commission's Draft Articles of State Responsibility.[11] Acts committed by individuals belonging to an organ of a State (such as the military) and private individuals empowered by the State to act under domestic legal regimes are generally held to be attributable to a State.

2. In the cyber context, determining legal attribution can be difficult and requires extensive intelligence inquiries into the relationship between the individual and the State in question. For example, a State's level of control over the individual or group is a key component. If a State provides only general guidance or training to a group engaging in malicious cyber operations against a foreign State, establishing legal attribution under the rules for State responsibility can be difficult. Direct control over key components of specific operations is generally required. Legal practitioners should be aware that this area of law is highly specialized, and legal attribution should never be assumed.[12]

III. Treaty Law

A. *Jus ad bellum:* United Nations (UN) Charter

1. The U.S. is a signatory to the UN Charter, the primary international agreement governing interactions among States. Article 2(4) of the Charter requires that all member States "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."[13]

   a) Most States and scholars interpret this language as prohibiting States from using force against another State unless excepted by another provision of law, such as self-defense. The UN Charter does not define the phrase *use of force*, although traditional interpretations include a requirement of violent action. Thus, it is generally accepted that some threshold of gravity must be crossed to constitute a use of force.[14] This precept has raised the critical question of whether a nonviolent but highly harmful cyber operation (e.g., attacks on financial or medical institutions) could constitute a use of force.

   b) U.S. policy was first articulated by former State Department legal advisor Harold Koh, who said that cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as uses of force.[15] Paul Ney's statement in 2020 was similar, maintaining that a cyber operation resulting in physical injury or damage that would be equivalent to a use of force in a more traditional context could violate art. 2(4). The DOD *LOWM* provides the examples of triggering a nuclear

plant meltdown, opening a dam over a populated area, or disabling air traffic control services as acts that would likely constitute a 2(4) violation.[16] The U.S., however, has not expressed a firm opinion on whether nonphysical effects could ever qualify as such. Other States are beginning to express their opinions on this subject (see table 2.1 at the end of this chapter), but nothing yet approaches international consensus.

2. There are two exceptions to the prohibition on the use of force: self-defense and a UN Security Council resolution pursuant to Chapter VII of the UN Charter.[17] It is the position of the U.S. that all illegal uses of force constitute armed attacks for the purposes of Article 51 of the UN Charter.[18] However, legal practitioners should understand that this interpretation is an isolated view, with the majority of States characterizing armed attacks as only "the most grave forms of the use of force."[19] Thus, it is the U.S. position that should a State violate the prohibition on the use of force, the victim-State would be justified in responding with force under Article 51. Additionally, the UN Security Council could authorize a coalition to use force under Article 42.

B. *Jus in Bello*: Geneva Conventions and Their Additional Protocols

1. Should multiple States or armed groups enter into armed conflict, then *jus in bello*—the rules governing the conduct of armed conflicts—will apply. The purpose of *jus in bello* is to prevent or mitigate serious harm to civilians or noncombatants and avoid the inhumane treatment of combatants and noncombatants. *Jus in bello*, the law of armed conflict, the law of war, and international humanitarian law are all largely synonymous terms. This body of treaty law in modern times comes primarily from the four Geneva Conventions and the Additional Protocols (AP) that followed. As with the UN Charter, all countries are parties to the Geneva Conventions, and most States are party to at least one if not all APs. The U.S. is not a party to AP I but still treats most of its provisions as customary international law.[20] The U.S. will exercise applicable *jus in bello* rules as a matter of policy (not law) even if a cyber operation does not implicate the appropriate body of law.[21]

2. Attacks

a) Perhaps the most challenging debate within the law of war regarding cyber operations is determining when a cyber operation with nonphysical effects constitutes an "attack." According to the DOD *Law of War Manual*, "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."[22] This determination is significant because an attack is the condition set for the application of targeting laws. For example, if there is no attack, for the purpose of the LoW, the principle of distinction would not apply. The wording here is essential, as AP I art. 49(1) defines *attacks* as "acts of violence against the adversary, whether in offence or in defence." The *Tallinn Manual* IGE drew heavily on this language when they defined a *cyberattack* in their Rule 92 as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[23]

b) In the *LOWM*, the DOD provides no clear standard for what would constitute an attack in cyberspace. It does, however, give some examples and factors to consider. For instance, § 16.5.1 states "a cyber attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure." Further, § 16.5.2 distinguishes "whether the operation causes only reversible effects or only temporary effects," which would weigh against that operation being considered an "attack." This distinction implicates the question of functionality. There is a small, but growing, number of States asserting that causing the loss of intended functionality, even where physical effects are not present, may constitute an attack for purposes of the LoW. Although the Tallinn IGE achieved no consensus on this subject, a majority agreed with this basic assertion.

3. Status of Data

   a) One fundamental consideration in the LoW is if electronic data constitutes an object for the purposes of the LoW, whether a military objective or a protected civilian object. If the target of an operation does not qualify as a person or object, then there is no requirement to observe most targeting rules (certain objects, such as hospitals, receive additional [special] protections). The argument in favor of categorizing electronic data as an object relies on the traditional LoW understanding of an object as "something that is visible and tangible."[24] This view is unlikely to include electronic data as constituting an object for LoW purposes. The counterargument takes a more flexible approach to the meaning of an object and invokes the "general rule" of interpretation in the Vienna Convention on the Law of Treaties (VCLT), Article 31(1), finding that a "treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose," and, therefore, given the importance of data in the modern age, the definition of a military objective should, in the digital age, include data targets.

   b) This question has been explored in depth by several prominent scholars and the *Tallinn Manual* IGE. The majority of the IGE found "that the law of armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law."[25] However, several prominent scholars disagree with this interpretation and believe a present-day understanding of objects should include electronic data.[26] Again, the United States has yet to express a formal position regarding this question.

4. LoW Principles. AP I lists the primary rules for armed conflict, but most rules may be categorized within five main principles: necessity, proportionality, distinction, humanity, and honor. While the LoW does not apply outside the existence of an armed conflict, the DOD position is that the U.S. will apply the LoW in all armed conflicts, regardless of how they are characterized, and act consistently with fundamental LoW principles and rules in all other military operations.[27] Armed conflicts are generally characterized as international armed conflicts (IAC) when two or more States are engaged in hostilities or as a non-international armed conflict

(NIAC) when at least one of the parties is a non-State armed group (such as al-Qaeda). Although there are significant legal differences between the two types of armed conflicts, the general principles of the LoW apply to both. Just as applying *jus ad bellum* principles to the use of force is difficult in cyber, it can be equally challenging to apply LoW principles in cyber.

a) Necessity.[28] This principle highlights that there must be a need to attack a particular target. Necessity allows the use of all measures required to defeat the enemy as quickly and efficiently as possible if not otherwise prohibited by the law of war. In essence, there must be some military advantage that is gained by attacking a particular military objective. *Military objectives* are defined in 10 U.S.C. § 950p(a)(1) as "combatants and those objects during hostilities which, by their nature, location, purpose, or use, effectively contribute to the war-fighting or war-sustaining capability of an opposing force and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of an attack." The last part of this definition invokes the principle of military necessity. Regarding cyber, the LoW requires that an attack on the targeted network, computer, domain, server, or controller provide a definite military advantage to the U.S. in the circumstances ruling at the time.[29] If the operation does not qualify as an attack, the DOD may nevertheless choose to apply the principle of necessity as a matter of policy. DOD Directive 2311.01, *DoD Law of War Program*, states that members will continue to act consistent with the law of war's fundamental principles and rules, which include those in Common Article 3 of the 1949 Geneva Conventions and the principles of military necessity, humanity, distinction, proportionality, and honor.

b) Proportionality.[30] This principle states that even when a State is justified in acting, it should not act in a manner that is excessive or unreasonable. Specifically, militaries must refrain from launching attacks expected to cause incidental loss of life or injury to civilians or collateral damage or destruction of civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated. Thus, the law provides a sliding scale as opposed to a binary determination. *Weaponeering*

is "the process of determining the quantity of a specific type of kinetic or non-kinetic means required to create a desired effect on a given target."[31] As a matter of policy, the DOD seeks to avoid damage or inconvenience to civilian networks when conducting cyberspace operations. However, given the frequent use of civilian cyber infrastructure by militaries, making a proportionality determination can be difficult. However, the DOD *LOWM* in § 16.5.1.1 states that "remote harms and lesser forms of harm, such as mere inconveniences or temporary losses, need not be considered in applying the proportionality rule." Like a collateral damage estimate on the kinetic side, collateral effects estimates are applied in cyberspace operations to determine how much, if any, civilian damage or injury will result from a cyberattack. The related principle of feasible precautions requires that the employment of cyberattacks should seek to minimize harm to civilian infrastructure and users to the extent possible, even when those operations comply with all other targeting rules.[32]

c) Distinction.[33] This principle requires that parties to a conflict distinguish between the armed forces and the civilian population (as well as protected objects and facilities). States are prohibited from attacking civilians or noncombatants. The definition of *military objective* becomes relevant here as well: "*objects which by their nature, location, purpose or use make an effective contribution to military action* and whose total or partial destruction, capture, or neutralization . . . offers a definite military advantage" (emphasis added).[34] In the cyber realm, it can be difficult to attempt to specify enemy servers or network devices. It becomes incumbent upon attorneys to coordinate with their operators and intelligence providers to distinguish between an otherwise civilian entity and the military contribution.

d) Humanity/Unnecessary Suffering.[35] This principle prohibits the infliction of suffering, injury, or destruction that is unnecessary to accomplish a legitimate military purpose. As stated in the necessity principle, States should act as quickly and efficiently as possible to defeat the enemy. They should not extend the destruction or suffering of the enemy to achieve their objectives. This principle is not typically implicated in cyber operations because most operations do not injure or kill combatants. How-

ever, one should not forget this principle when contemplating a potential target that is widely used or provides necessary services to civilians, such as power plants, telephone providers, and medical facilities. An attack on any of these types of targets may be wholly justified as a matter military necessity, but if the effects are long-lasting, they can pose a threat to the health and safety of combatants and noncombatants alike.

e) Honor/Chivalry.[36] This principle contemplates a certain amount of fairness in combat and mutual respect between opposing military forces. It began with the traditional concept of chivalry and endures today in more limited aspects. The main restrictions in this principle are misusing protected signs (medical/chaplain), fighting while using the enemy's uniform, or killing or wounding a person by resorting to perfidy (using another person's reliance on the laws of war to their detriment).[37] Honor also demands the humane treatment of prisoners of war and the application of combatant status/privilege. It is important to note that the principle of honor does not prohibit ruses or trickery by an armed force. The use of camouflage, decoys, misinformation, and false operations are legal under the LoW. For example, the DOD *LOWM* § 16.5.4 states that "it would not be prohibited to disguise network traffic as though it came from enemy computers or to use enemy codes during cyber operations."

E. International Positions on Key Issues Related to Cyberspace Operations

1. As noted, several key international law positions related to cyber operations remain unsettled. In some cases, the United States has taken positions counter to its allies and partners in cyberspace. In other instances, few States have provided any opinion or position related to these key issues. Understanding where State positions differ is vital when operating in a combined environment.

2. Table 2.1 shows the public positions of allied or partner States on various cyber issues. The content is not exhaustive for either the number of States providing positions or the scope of the positions offered. The table also summarizes or paraphrases often broad-sweeping and nuanced national political positions. Further, it is important to note that many national positions are evolving and may change rapidly. Ensure you consult the pertinent references when necessary to determine a State's exact position.

Table 2.1 State positions on key cyber questions

	Position					
Topic	**United States[a]**	**New Zealand[b]**	**France[c]**	**Germany[d]**	**Netherlands[e]**	**United Kingdom[f]**
What constitutes the use of force in cyberspace?	If physical injury or damage.	When scale or effects are equivalent to kinetic use of force.	Cyber operations without physical effects may constitute a use of force.	Look to scale and effects.	Cyber operations with serious financial or economic impact may qualify as the use of force.	Same criteria as kinetic operations.
Can cyber ops constitute armed attack in cyberspace?	The inherent right of self-defense potentially applies to any illegal use of force.	When effects are of a scale and nature equivalent to a kinetic armed attack.	When damage is of a significant scale or severity.	When effects are comparable to an armed attack, a State may exercise its right to self-defense.	When consequences are comparable to a kinetic armed attack (fatalities, damage, and destruction).	When resulting in or presenting an imminent threat of death and destruction equivalent to a kinetic armed attack.
Does the stand-alone rule of sovereignty apply to cyber operations?	Not sufficient and widespread State practice to find existence of such a rule.	Such a rule exists, but further State practice is required to determine its cyber application.	Yes, any cyber operation against digital systems or producing effects on foreign territory by digital means.	Unclear. However, it leaves open the possibility that the use of cyber capabilities might constitute a violation of sovereignty.	Yes, but only those breaches with a certain degree of infringement upon territorial integrity or when interfering with inherently governmental functions.	There is no stand-alone rule of sovereignty.
What constitutes an attack under the LoW?	Factors include whether the operation causes reversible or temporary effects.	Where it results in death, injury, or physical damage, including loss of functionality equivalent to that caused by a kinetic attack.	Where the targeted systems no longer provide the intended service. When temporary and/or reversible, when action is necessary to restore service.	Few official documents, but potentially applies to operations against certain critical infrastructure with indiscriminate effects or causing unnecessary suffering.	Few official documents, but specific rules regarding operations aimed at persons or objects apply equally to cyber operations carried out as part of an armed conflict.	No official State position at this time.

[a] Hon. Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020, https://www.defense.gov/.

[b] New Zealand Ministry of Foreign Affairs and Trade, "The Application of International Law to State Activity in Cyberspace," media statement, December 1, 2020, https://dpmc.govt.nz/.

[c] French Ministry of Armed Forces, *International Law Applied to Operations In Cyberspace* (Paris: Ministry of Defense, September 9, 2019), https://www.defense.gouv.fr/.

[d] Hon. Norbert Riedel, Commissioner for International Cyber Policy, German Federal Foreign Office, "Cyber Security as a Dimension of Security Policy" (speech, Chatham House, London, May 18, 2015), https://www.auswaertiges-amt.de/.

[e] The Netherlands Ministry of Foreign Affairs, letter to the Parliament on the international legal order in cyberspace, July 2019, https://www.government.nl/.

[f] Jeremy Wright, Attorney General, United Kingdom, "Cyber and International Law in the 21st Century" (speech, Chatham House Royal Institute for International Affairs, London, May 23, 2018), https://www.gov.uk/.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Department of Defense, *Law of War Manual*.

2. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*; and Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2d. ed.

3. Corn, "Tallinn Manual 2.0 – Advancing the Conversation"; and Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference."

4. DOD, *Law of War Manual*.

5. See Legal Status of Eastern Greenland (Denmark v. Norway), 1933 P.C.I.J. (ser. A/B) No. 53, at 71 (Apr. 5, 1933) (holding that a unilateral statement made on behalf of a country's government by its minister of foreign affairs may be binding on that country).

6. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment, 1986 I.C.J. [International Court of Justice] 14 (Jun. 27, 1986).

7. Tsagourias, "Electoral Cyber Interference."

8. Deeks, "Defend Forward and Cyber Countermeasures."

9. United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397.

10. Compare Schmitt and Vihul, "Sovereignty in Cyberspace?," 213, with Corn and Taylor, "Sovereignty in the Age of Cyber," 207.

11. "Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, 2001."

12. British Institute of International and Comparative Law, *State Responsibility for Cyber Operations: International Law Issues*.

13. Charter of the United Nations, Jun. 26, 1945, 59 Stat. 1031, at art. 2, para. 4 (hereafter cited as UN Charter).

14. Corfu Channel (U.K. v. Alb.), Judgement, 1949 I.C.J. Rep. 4, 35 (Apr. 9).

15. Koh, "Obama Administration and International Law."

16. DOD, *Law of War Manual*, § 16.3.

17. See UN Charter, arts. 42, 51.

18. See, for example, DOD, *Law of War Manual*, § 16.3.3.1.

19. See Nicaragua v. United States of America, 1986 I.C.J. 14, para. 228 (June 27).

20. DOD, *Law of War Manual*, §§ 19.20.1 and 19.20.2.1 (stating the reasons for not ratifying based on former president Ronald Reagan not agreeing with specific language included in APs I and II); and Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977.

21. Ney, "DOD General Counsel Remarks"; and DOD, *Law of War Manual,* § 1.2.a.

22. DOD, *Law of War Manual*, §§ 1.2.a and 16.1.3.2.

23. Schmitt, *Tallinn Manual 2.0*, 2d ed., rule 38, para. 5.

24. Sandoz, Swinarski, and Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987), para. 2008.
25. Schmitt, *Tallinn Manual 2.0*, 2d ed., rule 100, para. 6.
26. Mačák, "Military Objectives 2.0," 55.
27. DOD Directive 2311.01, *DoD Law of War Program*, para. 1.2(a).
28. See DOD, *Law of War Manual*, § 2.2.
29. DOD, *Law of War Manual*, § 5.7.7.
30. DOD, *LOWM*, § 2.4.
31. Air Force Doctrine Publication 3-60, *Targeting,* 50.
32. DOD, *Law of War Manual*, § 16.5.3.
33. DOD, *Law of War Manual*, § 2.5.
34. "Military Objectives," Cyber Law Toolkit.
35. DOD, *Law of War Manual*, § 2.3.
36. DOD, *Law of War Manual*, § 2.6.
37. Biller, "Misuse of Protected Indicators in Cyberspace"; and "Perfidy and Ruses of War," Cyber Law Toolkit.

Chapter 3

Intelligence Law Considerations for Cyberspace

I. Introductory Concepts

A. Cyberspace operations have their origin in the intelligence community (IC), with the Air Force developing its initial cyber capability at the then Air Intelligence Agency (now part of Sixteenth Air Force) and the greater IC doing the same at the National Security Agency (NSA).[1] Besides a common origin, cyberspace operations and certain intelligence activities are so operationally similar that it can be difficult to tell one from the other based solely on the techniques employed. These commonalities notwithstanding, the separation between cyberspace and intelligence operations is strictly maintained even when the two are part of the same command or when sharing the same commander/director as is the current case with U.S. Cyber Command (USCYBERCOM) and the NSA.

B. This separation stems from the distinctly different legal and policy regimes regulating intelligence and cyberspace operations. For example, intelligence activities are limited in purpose, with only foreign intelligence and counterintelligence (CI) permissible mission sets. These activities are also constrained by geography and target, with strict limits on the conduct of foreign intelligence within the United States and on the collection, retention, and dissemination of United States person information (USPI) regardless of where that person is located.

C. Extensive regulations also govern cyberspace operations, but the two regimes' legal and policy considerations have individual origins and focus. Thus, understanding the difference between cyberspace operations and intelligence activities is essential to properly applying governance regimes. Once the "intelligence activity" determination has been made, a legal advisor must know how to determine a permissible activity. To these ends, the following sections begin by defining *intelligence activity* and then outlining the parameters of a fundamental intelligence legal analysis. Next is an overview of intelligence issues that legal advisors will likely encounter when supporting information warfare or cyberspace operations units.

II. What Is an "Intelligence Activity"?

A. Defining *intelligence activity* is the first step toward determining the activities regulated by intelligence law and policy. Executive Order (EO) 12333 is a foundational source of U.S. Government intelligence authority.[2] It defines *intelligence activities* in a somewhat circular way as all activities EO 12333 authorizes U.S. Government elements to conduct.[3] This definition is vague, but a closer examination of EO 12333 narrows the scope of "intelligence activity" and gives it a more precise meaning.

B. EO 12333 begins this clarification by defining *intelligence* in its preamble as "timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents." It then separates intelligence into two disciplines: foreign intelligence and counterintelligence, the definitions of which inform the types of "timely, accurate, and insightful information" that may be permissibly sought.[4] With these definitional boundaries set, EO 12333 authorizes specific elements of the U.S. Government to conduct particular types of foreign intelligence and CI activities. In turn, these authorizations define what *intelligence activity* means for the organizations to which the authority is given.

C. Two such authorizations define *intelligence activity* for the DOD.

1. The first is in EO 12333, Sec. 1.7(f), authorizing the head of each Service's IC element to "collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related [foreign] intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements."

2. The second is in EO 12333, Sec. 1.10(a)-(c), authorizing the secretary of defense (SecDef) to "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence" and to "collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities."

3. Given that an "intelligence activity" is anything EO 12333 authorizes, it follows that collection, production, analysis, and dissemination are all intelligence activities. Joint doctrine further defines

the term by adding "processing, integration, evaluation, analysis, and interpretation of available information" in place of "analysis" and "production."[5] Accordingly, for DOD purposes, an *intelligence activity* is an action involving the collection, processing, integration, evaluation, analysis, interpretation, or dissemination of foreign intelligence or counterintelligence within the scope of Presidential authorizations in EO 12333.

D. Whether a particular military action is an intelligence activity is often straightforward. However, the reality is that the intelligence-activity-or-no determination can be nuanced. There are no set criteria for making these determinations. Still, Department of the Air Force (DAF) attorneys have for many years used the so-called 6 Ps Test to determine whether a domestic imagery mission triggers intelligence oversight requirements and approval levels. A variation of the 6 Ps Test (with a seventh added) can help distinguish intelligence activities from cyberspace operations.[6] The Ps are factors that clarify the nuances of a proposed activity, which in turn aids the intelligence-activity-or-no determination.[7]

1. The first P is *Permission*. This factor focuses on the line of authority relied upon for conducting the activity. The inquiry can begin and end with this P, which states that an action that closely resembles an operational activity is likely an intelligence activity if it relies on an intelligence authority for permission. It is when permission could follow an operational or intelligence path that further inquiry is most likely necessary.

2. The second P is *People*. Is the task performed by an intelligence professional or intelligence unit? Under what line of authority is the person/unit performing the activity? This factor alone is not determinative, as non-intelligence personnel can perform intelligence activities if authorized, but the person or unit's profession is a helpful indicator.

3. The third P is *Purpose*. In the military, the purpose of intelligence is typically to provide information on "foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations" that commanders need to conduct assigned responsibilities or prepare for the future execution thereof.[8] Does the proposed military action require, for example, collection, processing, and integration of this type of information to inform a commander's

decisions about a foreign adversary? If not, what purpose does it serve—public health, operations security, cybersecurity, or some other operational purpose?

4. The fourth P is *Pipes*. Will the activity result in a product placed on an intelligence directorate's online portal? Will the information acquired during the activity be entered into intelligence databases for evaluation, or will the finished product (often a report) be entered into intelligence repositories for use by the broader IC? Does the performance of the activity require access to intelligence databases and resources?

5. The fifth P is *Process*. This factor examines how information moves from proposal to fruition. Does the activity require knowledge of intelligence sources or methods? Is it the product of an intelligence planning process? Does the activity require the participation of an IC element to acquire the data or process, analyze it, and create products from it? Or is this a military action that non-intelligence personnel and units do routinely without specific intelligence support or access?

6. The sixth P is *Platform*. This factor considers the activity's required equipment and whether it is owned or operated by an intelligence unit. If not, will the activity require the use of a non-intelligence platform for an intelligence purpose? For example, the targeting pod on strike aircraft is not an intelligence platform, but it is conceivable that it might be used for an intelligence purpose.

7. The seventh and final P is *Procurement*. This factor considers who paid for any equipment needed for the activity. Was it procured using Military Intelligence Program or National Intelligence Program funds? Or was it from operations and maintenance or some other non-intelligence source of funding?

E. In summary, examining the proposed activity and its underlying authority often leads to a clear determination of whether it should be categorized as an intelligence activity. However, when circumstances are unclear, the 6 (+1) Ps test can inform and animate the definition of an intelligence activity, thus helping legal advisors make a correct determination. When applying the elements of the 7 Ps Test, legal advisors should keep the following in mind:

1. First, intelligence law and policy follow the activity, not the profession of the person performing it.[9] Consequently, an activity that a non-intelligence unit or person performs does not automatically fall into the non-intelligence category. The status of personnel and units is thus relevant to the calculus but is not determinative.

2. Second, the factors of the 7 Ps Test should be weighed and balanced holistically rather than individually. For example, the Joint Worldwide Intelligence Communications System (JWICS) is an intelligence network also used for operational purposes. Its use does not transform a cyberspace operation into an intelligence activity. The same is true for *Platforms* in that capabilities may be useful for intelligence activities and cyberspace operations. A holistic approach is thus necessary, but some factors may be weightier than others, such as *People*, *Permission*, and the activity's *Purpose*.

3. Finally, while the 7 Ps Test helps parse the small facts on which analysis often turns, the factors do not replace the definition of *intelligence activity*. In short, the definition is the standard, and while the 7 Ps Test animates the standard, the conclusions must reflect the definition.

III. Tracing Intelligence Authority

A. Assuming the military action under review is an intelligence activity, the next step is determining whether it is a permissible one. Rules governing intelligence activities fall into two general categories: positive law authority to undertake intelligence activities and restrictions on activities involving the collection, retention, and dissemination of USPI. The positive law aspects are analyzed first, followed by restrictive components collectively known as intelligence oversight.

B. Positive Law Permissibility

1. Intelligence personnel undertake intelligence activities to provide information relevant to a commander or other government official's request for information, also known as an intelligence requirement. To determine the permissibility of an intelligence activity, one must establish if the unit or person seeking to answer an intelligence requirement has the authority to do so.

2. Understanding how intelligence authorities work first requires insight into the governing legal regime. Legal regimes are normally either permissive or restrictive. Under a permissive legal regime, a person may act freely unless the activity is expressly prohibited. Restrictive regimes are the opposite, meaning a person is free to engage in a particular activity if, and only if, it is expressly authorized.[10]

3. Intelligence law fits neither model. Rather, it is quasi-restrictive, meaning that intelligence activities require positive authority but usually not specific authorization at high levels. That is, positive authority is required, but permission typically comes through broadly worded statements versus a definitively worded authorization for specific intelligence activities (covert action is a notable exception to this general rule). Positive authority to execute an intelligence activity is, of course, only as good as the authority that backs it up, meaning the person authorizing the activity must have the authority to do so.

4. To determine permissibility, it is necessary to find the immediate source of intelligence authority and to continue tracing the line of authority back to its origin. For intelligence activities performed by the U.S. Government, tracing "go do" authority for an intelligence activity means finding a positive link to the President's authority, with its source in Article II of the U.S. Constitution.[11] This is not to say that Congress has no impact on intelligence activities. Evaluating Title 10 and Title 50, Chapter 44, of the U.S. Code reveals that Congress has considerable authority over the conduct of intelligence activities, their funding, and the reporting of information to Congress. However, for "go do" intelligence authority, one must look to the President's constitutional powers.

5. Sources of Presidential Intelligence Authority

    a) The President's intelligence authorities are derived from two constitutional sources. The first is the "vesting clause" in which the President is vested with the United States' executive power.[12] The second is the clause naming the President the "Commander in Chief of the Army and Navy" and, by implication, the rest of the military Services and branches.[13] As the "sole organ of the federal government in . . . international relations" and the ultimate military commander, the President's enumerated powers

include authority to form foreign and national security policy and determine how best to employ American military power.[14]

b) The performance of these functions is helped substantially by information about the foreign States with which the President deals and against which his subordinate forces sometimes fight. Fortunately for the President, the authority to acquire information necessary to execute Presidential responsibilities has been long considered an inherent part of the executive branch's enumerated powers.[15]

c) From this inherent authority are born the intelligence elements of various U.S. Government departments and agencies and the Presidential and departmental policies authorizing and governing the conduct of those activities. The most important of these directives is EO 12333, which defines *intelligence*; authorizes IC elements to conduct intelligence activities; and outlines the authority and responsibilities of executive branch department heads, IC element heads, and IC elements.

6. Intelligence Authority in the Department of the Air Force

a) EO 12333 includes Presidential grants of authority to "Intelligence Community Elements," a group that includes each of the Services' foreign intelligence and counterintelligence elements.[16] The portion of EO 12333 relevant to the Services specifically authorizes the "Commanders and heads" of the Service IC elements to "collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related [foreign] intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements."[17] This provision's practical impact is in providing the Air Force IC element and the new Space Force IC element—meaning Service-retained intelligence units and personnel—the authority to conduct intelligence activities consistent with this grant of authority. Importantly, within the DAF are the Air Force and the new Space Force intelligence elements that are separate and distinct members of the IC. This primer focuses on the Air Force intelligence element due to the role and responsibilities of the Deputy Chief of Staff of the Air Force for Intelligence, Surveillance, and Reconnaissance and Cyber Effects Operations—better known as the Director, Headquarters Air Force/A2/6 (HAF/A2/6).

b) An interesting aspect of this authority is that while the Secretary of the Air Force is responsible for the "effective supervision and control" of Air Force intelligence activities, the authority to conduct those activities, and thus to authorize them, goes directly from the President, in coordination with the Office of the Director of National Intelligence, to the head of each Service's IC element.[18] The Director of National Intelligence, a cabinet position, is the head of the IC and responsible for promulgating its national policy.[19] In the Air Force's case, the head of the IC element is the Director, HAF/A2/6.[20] Thus, the incumbent may authorize and direct the Air Force IC element's intelligence activities, provided they are consistent with the authority given in EO 12333, Sec. 1.7(f).

c) The Director, HAF/A2/6, uses this authority to set intelligence policy for the Air Force and to define units' authorized intelligence activities. For example, the Air Force Office of Special Investigations (AFOSI) is the Air Force's counterintelligence element and the only Air Force organization authorized to conduct CI activities.[21] This grant of authority to the AFOSI was issued by HAF/A2/6.

d) HAF/A2/6 has also directed Air Combat Command (ACC) to lead "integration of multiple source and discipline ISR across all domains" and to develop "sensor- and discipline-agnostic ISR processing, exploitation, and dissemination work centers focused on [the] commander's priority intelligence requirements."[22] Though ACC is not an element of the IC per se, this grant of authority authorizes it to set policy and define subordinate IC units' intelligence authority. Subordinate units receiving these authorizations can, in turn, direct and manage the intelligence activities of their organizations. This process of passing intelligence authority from one echelon to the other continues to the point of intelligence activity execution.

e) Knowing where to look for these authoritative links is the key to determining an intelligence activity's permissibility. Technically, the entire Air Force intelligence element has a grant of authority under EO 12333, Sec. 1.7(f). However, this broad authority may be restricted as it devolves from HAF/A2/6 to command echelons.

f) An attorney advising the Air Force intelligence element must therefore begin with EO 12333's grant of authority and then look to HAF/A2/6 issuances for authoritative statements applicable to the advised unit, either directly or through the authoritative direction of an intervening headquarters. It is also useful to look to the *Intelligence Community Legal Reference Book*.[23] If authoritative links to the Constitution can be established and if the intelligence activity is consistent with the unit's grant of authority, then the intelligence activity is likely a permissible one. However, it remains subject to intelligence oversight requirements, congressional restrictions and authorizations, and, as discussed later, IC agency policy.

7. Intelligence Authority in the Combatant Commands

a) The flow of intelligence authority to combatant commands (CCMD) is more circuitous than for Air Force intelligence elements. This is because CCMDs are not IC elements and do not receive intelligence authority directly from the President. Instead, intelligence authority flows to the CCMDs in the same way operational authority does: from the President to the SecDef and then down to the CCMDs.

b) In EO 12333, Sec. 1.10, the President outlines the intelligence authorities and responsibilities of the DOD, expressly authorizing the SecDef to "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence"; to "collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities"; and to "conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements."[24]

c) The President has authorized the SecDef to use DOD IC elements to execute these authorities and has also authorized the use of "other departments, agencies, or offices within the [DOD], as appropriate, to conduct the intelligence missions and responsibilities assigned to [the SecDef]."[25] CCMDs are not IC elements, but they are "other departments, agencies, or offices" within the DOD. Accordingly, the SecDef can provide

CCMDs with authority to conduct intelligence activities consistent with the SecDef's grant of Presidential authority.

d) This intelligence authority normally flows from the SecDef to the CCMDs through an execute order (EXORD) or deployment order (DEPORD) that gives a combatant commander (CCDR) an assigned mission along with authority to accomplish it.[26] The authority to accomplish an assigned mission is accompanied by the inherent command authority to use subordinate intelligence personnel and assets to that end, but intelligence authority can also be expressly addressed in the EXORD/DEPORD. Additionally, a specified intelligence authority may come in a standalone SecDef memorandum or other document in which the SecDef or a delegee has authorized a particular type or category of intelligence activities. Thus, while EXORDs and DEPORDs are typical, assigned missions and intelligence authorities can flow from the SecDef in various ways. Once intelligence authority is passed to a CCMD, it is typically given to lower echelons through operation orders (OPORD) or other military order through which CCDRs assign missions and grant authority to subordinate commanders and forces. This process can continue to lower command echelons down to the point of intelligence activity execution.

e) Staffing practices, orders development, and even what the orders are called can vary. However, regardless of process or format, a common thread is that intelligence authority is always passed through orders issued by someone with authority to grant it. For an intelligence activity in a CCMD to be proper, military orders from a person authorized to give them must form a link between the intelligence activity and the CCDR's authority, as well as further links back to the SecDef and the constitutional powers of the President. If these links exist and the intelligence activity is consistent with their authoritative parameters, then there is a positive authority for the intelligence activity, and it is likely permissible—subject to intelligence oversight requirements, additional restrictions from Congress, and IC agency policy.

8. The Role of Other U.S. Government Agencies

a) The above description of intelligence authorities and how they flow is useful as a rule. However, it paints an incomplete picture because it does not account for the roles of other U.S. Government organizations. The IC comprises eighteen organizations, five of which are in the military Services (DAF elements are the Air Force intelligence element and Space Force intelligence element).[27] The other thirteen perform missions and functions given to those organizations by the President in EO 12333, some of which affect the U.S. Government or DOD as a whole.

(1) The Defense Intelligence Agency (DIA) is the "DOD lead for coordinating intelligence support to meet [CCMD] requirements; lead efforts to align analysis, collection, and Intelligence, Surveillance, and Reconnaissance (ISR) activities with all operations; and link and synchronize Military, Defense, and National Intelligence capabilities."[28] The DIA has also been tasked with centrally managing the DOD's human intelligence (HUMINT) enterprise.[29] Thus, DIA policy may apply to any DOD organization conducting HUMINT activities.

(2) The NSA also has sweeping authorities and responsibilities that apply not just to the DOD but the entire U.S. Government. As the lead agency for signals intelligence (SIGINT), the NSA is responsible for developing and operating a unified organization for SIGINT activities, issuing regulations for their conduct, and exercising SIGINT operational control (OPCON) over the SIGINT activities of the U.S. Government.[30] Additionally, the President named the NSA director (DIRNSA) as the SIGINT functional manager for the U.S. Government, and the SecDef has delegated DIRNSA the authority to "authorize another [U.S. Government] department or agency to engage in SIGINT activities in coordination with the DNI."[31] These provisions collectively mean that any U.S. Government organization conducting SIGINT activities is doing so with DIRNSA's approval and authority and is obligated to follow NSA's operational direction and its training, tradecraft, and operational policies.

b) The key takeaway from this section is that while the flow of authority described in the Air Force intelligence element and

CCMD sections is generally true, the type of intelligence activity being performed may require a legal advisor to look outside of an organization when tracing intelligence authority. Further, even if not the source of authority, outside agencies may have a say in the training and equipping of the Air Force intelligence element and CCMDs and the conduct of certain intelligence activities.

9. The Role of Congress

   a) Discussion on how to trace intelligence authority has thus far focused on the "go do" authority of the President. While understanding how intelligence authority flows downward is of paramount importance, a legal advisor must also be aware of how congressional authority affects intelligence activities.

   b) Congressional intelligence authority stems from Congress's constitutional powers. Article I, Sec. 8, gives Congress the power to "provide for the common Defense," to raise and support an Army and provide and maintain a Navy, and to make "Rules for the Government and Regulation of the land and naval forces."[32] Along with these enumerated powers, Congress also has the power to enact legislation "necessary and proper" to carry out its constitutional functions.[33] Information about foreign States is critical to the "common defense" and the conduct of military operations. Therefore, it follows that authority to authorize and fund intelligence units and capabilities and regulate the scope of authorized intelligence activities is an inherent part of Congress's enumerated powers. For example, in Section 3 of the National Security Act (50 U.S.C. §3003), Congress statutorily defines *intelligence*, *foreign intelligence*, and *counterintelligence*; in Section 501 of the National Security Act, it specifies accountability measures for executive branch intelligence activities.[34]

   c) The key takeaway here is that while "go do" intelligence authority flows from Presidential authority through EO 12333, Congress has much to say on how intelligence activities are conducted, how funding may be spent, and who is responsible for ensuring intelligence activities comply with law and policy. Accordingly, in addition to tracing Presidential authority and determining how IC policy may affect the conduct of a particular intelligence activity, a legal advisor must also be aware that con-

gressional action may circumscribe that activity and perhaps dictate the level at which it may be approved.

C. Restrictive Permissibility (Intelligence Oversight)

1. The second component of permissibility is intelligence oversight, a body of law and policy that governs and restricts the conduct of intelligence activities and provides congressional oversight. Intelligence oversight as a matter of law—meaning congressional oversight—is straightforward from a statutory language perspective. Congress requires the President to keep its intelligence oversight committees "fully and currently informed of the intelligence activities of the United States" and to "promptly" report any illegal intelligence activities.[35] Besides this general intelligence oversight requirement, Congress also requires written Presidential approval for any covert action and the reporting of covert actions to the intelligence committees.[36]

   a) While straightforward in their terminology, these statutory provisions can be complex in application. For instance, intelligence activities that initially appear covert may instead be clandestine, and what appears to be an intelligence activity may instead be a military operation subject to different reporting and oversight requirements. Additionally, telling Congress about every intelligence activity the U.S. Government conducts would be administratively burdensome for all parties, which begs the question of what keeping Congress "fully and currently informed" really means.

   b) For a robust discussion of statutory intelligence oversight and its intricacies, see Professor Bobby Chesney's article "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate."[37] For a similar discussion from a former U.S. Special Operations Command attorney, see Andru Wall's article "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action."[38] Also see BG Joseph Berger's discussion of covert action and the chain of command in his article "Covert Action: Title 10, Title 50, and the Chain of Command."[39]

2. Intelligence Oversight as a Matter of Policy

   a) Intelligence oversight as a matter of policy (the type on which most legal advisors spend their time) is an executive branch creation born out of congressional investigations into IC activities from the 1950s through the early 1970s. In the aftermath of these investigations, President Gerald Ford issued Executive Order 11905, and in doing so circumscribed the scope of intelligence activities the IC is permitted to perform. These initial ground rules were followed by EO 12036, issued by President Carter, and EO 12333, issued by President Reagan. EO 12333, as amended, remains in force today. While much of it focuses on IC elements and the scope of intelligence authority given to each, it is also the source of intelligence oversight policy for the executive branch.

   b) Intelligence oversight policy in EO 12333 recognizes two distinct and potentially competing interests: (1) the privacy interests of individuals and organizations protected by United States law and the Constitution and (2) the need for policy makers and military commanders to have timely and accurate information to do their jobs. Intelligence oversight seeks to balance these interests by recognizing there are times when it is necessary to collect, retain, and disseminate USPI but restricting those times to certain circumstances and requiring elevated approval levels for some activities and locations.

   c) EO 12333 also requires executive branch department heads to implement intelligence oversight policy within their organizations. The SecDef has done so for the DOD through a family of four documents. DOD Directive 5240.01 assigns responsibilities and provides the basic parameters of DOD intelligence oversight policy.[40] DOD Manual (DODM) 5240.01 implements this directive by providing procedures to govern the conduct of Defense Intelligence Components and non-intelligence components or elements, or anyone acting on behalf of those components or elements, when conducting intelligence activities under DOD's authorities. The manual defines *Defense Intelligence Components* as all DOD organizations that perform foreign intelligence or CI missions or functions.[41] DOD Regulation 5240.01-R provides three additional procedures that govern

contracting for goods and services, intelligence support to law enforcement, and human experimentation for intelligence purposes.[42] Finally, DOD Directive (DODD) 5148.13 assigns intelligence responsibilities to various DOD officials and outlines the procedures for identifying, investigating, and reporting questionable intelligence activities (QIA) and significant or highly sensitive matters (S/HSM).[43]

d) Each of these documents is an integral component of intelligence oversight policy, but most legal advisors will spend their time primarily in DODM 5240.01. Its procedures, definitions, and other important terms will not be restated here, as there is no substitute for digging into the document. However, the following provisions are worth highlighting:

(1) Intelligence oversight follows the activity, not the profession (DODM 5240.01, para. 3.1.a.[1]). Consequently, that a person or unit is not "intel" does not necessarily dispose of intelligence oversight requirements. The unit's activities, their purpose, and the line of authority directing them—along with the rest of the 7 Ps Test—determine intelligence oversight applicability.

(2) Many components of intelligence oversight policy are classified.[44]

(3) Intelligence oversight applies differently to intentionally collected USPI than it does to USPI collected incidentally, and it distinguishes USPI collection occurring inside the United States from that which occurs outside of it.[45] USPI collected intentionally is particularly restrictive and is permitted only when reasonably believed necessary to perform a mission or function assigned to the unit and when it falls within one of thirteen enumerated categories. Intentional versus incidental collection and where it occurs can also affect the approval authority for the intelligence activity and how long the data can be retained for analysis.[46]

(4) USPI must be collected using the least intrusive means feasible, from publicly available information to collection techniques that require a judicial warrant or permission from the U.S. Attorney General, with a couple of steps in between.[47]

IV. Putting It All Together—Conducting the Analysis

A. Reviewing an intelligence activity for legal sufficiency consists of applying the components discussed above. The initial step in any analysis is determining whether the action in question is an intelligence activity. If it is, the analysis moves on to whether it is a permissible one.

B. Permissibility has two components. The first focuses on whether the unit or person has authority to conduct the intelligence activity—what intelligence professionals often refer to as having the "mission" to do the activity. The authority analysis typically consists of determining whether (1) the intelligence activity fits the definition of foreign intelligence or counterintelligence, (2) someone with proper authority has authorized the intelligence unit to conduct that particular type of activity, and (3) the activity is consistent with that grant of authority. Looking for these authoritative links necessarily depends on whether one is advising a Service IC element unit or a unit with a command relationship with a CCDR. Assuming "go do" intelligence authority can be found, congressional intelligence authority and DOD policy may shape how the intelligence activity can be conducted.

C. The second component of permissibility involves whether the intelligence activity requires collecting, retaining, and disseminating USPI. If so, the activity is allowable only in accordance with the procedures in DODM 5240.01 and DOD 5240.01-R. Assuming the two components of the permissibility analysis are met, the intelligence activity is most likely authorized.

V. Potential Issues with Intelligence and Cyberspace Operations

A. Intelligence plays an essential role in planning and executing cyberspace operations. However, the confluence of the two is not always problem free. It can be rather complicated, and the following sections outline the types of issues legal advisors may see when advising an intelligence, cyberspace operations, or information warfare unit. The list is by no means exhaustive but rather a preview of issues an attorney may face.

B. The first potential issue involves data sets. Information is a valuable commodity that can be used across multiple disciplines. However, operational data sets are not intelligence data sets, and exploiting the

contents of an operational data set for intelligence purposes may or may not be permissible. For example, a cybersecurity data set may contain evidence of cybercrime, but that does not mean it also fits the definition of foreign intelligence or counterintelligence. On this subject, it is important to note that DODM 5240.01 addresses one problem with data sets by allowing Defense Intelligence Components to perform data-related tasks in shared repositories they host without triggering a "collection."[48]

C. The second potential issue is the use of publicly available information (PAI).

   1. DOD policy permits DOD organizations to "access, obtain, and use PAI to plan, inform, enable, execute, and support the full spectrum of DOD missions."[49] However, PAI cannot be used in any manner the organization wants. Defense Intelligence Components, for instance, must comply with DODM 5240.01 when acquiring PAI during intelligence activities.[50] DOD personnel not conducting intelligence activities must comply with Department of Defense Directive (DODD) 5200.27 when acquiring PAI related to persons and organizations not affiliated with the DOD.[51] Services and CCMDs may also have PAI-specific policies that apply to units and personnel subordinate to them.

   2. PAI-related issues may arise as part of the intelligence-activity-or-no analysis. Anyone answering a commander's request for information (typically an A3) might be using tools and processes that appear to be an intelligence activity. Another problematic area for PAI is that many non-intelligence personnel do not realize their acquisition of PAI is regulated by DOD and DAF policy. Intelligence oversight policy does not apply, but those activities are not regulation free (e.g., DODD 3115.18; Air Force Manual [AFMAN] 14-405).

   3. For personnel acquiring PAI as an intelligence activity, the issue becomes whether the data obtained is publicly available. PAI is a term of art defined in DODD 3115.18 and DODM 5240.01 as including information "accessible online or otherwise to the public."[52] This broadly worded statement seems to open the entire Internet to PAI acquisition and use. However, legal advisors must be aware that the scope of "is accessible online" is still being debated. How

much information can be collected as "PAI" can differ from one organization to the next as a matter of policy interpretation.

D. The third potential issue, and the one most likely to be fielded by an installation legal office, is intelligence support to mission defense teams (MDT). MDTs are covered in depth elsewhere in this primer, but for purposes of this discussion it is enough to note that MDTs are wing-level Service-retained units that may look to the intelligence flight in their local operations support squadron (also Service retained) for intelligence support. The question, then, is what kind of support can a local intelligence flight provide? That is, what is the scope of the intelligence authority under which local intelligence flights conduct intelligence activities?

   1. EO 12333 defines the *Air Force intelligence element* as those components of the Air Force that conduct foreign intelligence and counterintelligence.[53] Local intelligence flights are not counterintelligence units, but they perform activities relating to the "capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[54] They are an element that accomplishes foreign intelligence activities. Therefore, local intelligence flights are part of the Air Force intelligence element and are a recipient of IC element authority.

   2. As previously discussed, the Air Force intelligence element is authorized to "collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related [foreign] intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements."[55] This broad statement is the default scope of authority for Air Force intelligence element units. However, this authority can be circumscribed by higher command echelons, which is what has happened with local intelligence flights.

   3. The HAF/A2/6 director has made ACC the lead command for integrating "multiple source and discipline ISR across all domains" and responsible for developing an "ISR Fusion Warfare Concept of Operations that addresses . . . unit level functions."[56] Using this authority, ACC has published authoritative guidance to "Unit-level Intelligence" units, which it defines as "personnel who perform [Unit-level Intelligence] duties supporting AF operational

missions at wing level and below."[57] Thus, the intelligence flight is an operations support squadron. This guidance clearly applies to units within ACC, but given that ACC is the lead command for multi-source/discipline ISR for the Air Force, its requirements are arguably applicable across the department.

4. Through ACC Manual 14-402, ACC has authorized local intelligence flights to directly support MDTs in three areas: training, mission planning support, and threat analysis.[58] ACC does not elaborate on the scope of this intelligence authority, but it is notably identical to the authority given for intelligence support to force protection on which ACC does elaborate. Accordingly, the sections of ACC Manual 14-402 addressing support to force protection (chap. 5) inform what support may be provided to MDTs.

5. The above guidance suggests that intelligence support to MDTs, unless the flight has additional authority from elsewhere, does not include collection activities.[59] Rather, it is limited to producing intelligence products from existing intelligence reports and analyzing information already collected by someone else. Perhaps most important is that this authority does not permit on-network intelligence activities. Such activities are cybersecurity functions when performed by MDTs for an operational purpose. However, when conducted as an intelligence activity they are a form of SIGINT. "Blue space" SIGINT is governed by Foreign Intelligence Surveillance Act (FISA) processes and is strictly prohibited outside of those parameters. Accordingly, while intelligence personnel may accept information from cooperating sources (like MDTs) and then analyze that information for foreign intelligence purposes, they are not themselves permitted to conduct on-network operations.[60] Lastly, it is important to remember that intelligence support provided to MDTs must have a foreign nexus; local intelligence flights are foreign intelligence units and may *not* stray outside of this lane when conducting intelligence activities.

E. The final potential issue involves the unauthorized mixing of authorities in commands with a multi-hatted commander. This issue is not unique to cyber and intelligence. Still, the risk of crossing lines of authority is especially acute in an "information warfare" unit like Sixteenth Air Force where the commander wears five distinct hats, two of which are subordinate to a CCMD and one subordinate to a DOD

intelligence agency. Staff and planners can work closely together and collaborate on common problems, but legal advisors must have a firm grasp of the current command relationships especially in the context of Sixteenth Air Force (Air Forces Cyber [AFCYBER]).

F. Much of the discussion relative to the authorities and command responsibilities is controlled unclassified information (CUI) and is not publicly releasable. Consequently, we recommend contacting ACC/JA or 16 AF/JA for further information.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Hayden, *Playing to the Edge,* 127–52.
2. EO 12333, United States Intelligence Activities.
3. EO 12333, as amended July 30, 2008, Sec. 3.5.(g).
4. EO 12333, as amended, Secs. 3.5.(a), 3.5(e), 3.5(f).
5. Joint Publication (JP) 2-0, *Joint Intelligence,* GL-08.
6. Zoldi, "Protecting Security and Privacy," 22.
7. See Air Combat Command Instruction (ACCI) 10-810, *Operations Involving Domestic Imagery Support Request*.
8. JP 2-0, *Joint Intelligence*, GL-8, s.v. "intelligence."
9. See DOD Manual (DODM) 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, paras. 1.1 and 3.1.(a)(1).
10. Whitaker, "Intelligence Law," 519.
11. Whitaker, 520.
12. U.S. Const. art. II, §1.
13. U.S. Const. art. II, § 2.
14. *U.S. v. Curtiss-Wright Corp*, 299 U.S. 304, 320 (1936).
15. In the case of *Totten v. United States*, 92 U.S. 105, 106 (1876), the Court states, "We have no difficulty as to the authority of the President in the matter. He was undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy; and contracts to compensate such agents are so far binding upon the government as to render it lawful for the President to direct payment of the amount stipulated out of the contingent fund under his control." In the case of *Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp.* 333 U.S. 103, 111 (1947), the Court recognized without comment that "the President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world." John Yoo states, "The ability to collect intelligence is intrinsic to

the use of military force. It is inconceivable that the Constitution would vest in the President the powers of Commander-in-Chief and Chief Executive, give him the responsibility to protect the nation from attack, but then disable him from gathering intelligence to use the military most effectively to defeat the enemy." Yoo, "*Legality of the National Security Agency's Bulk Data Surveillance Programs*," 321.

16. EO 12333, United States Intelligence Activities, Sec. 1.7.

17. EO 12333, Sec. 1.7(f).

18. See EO 12333, Sec. 1.7(f); and 10 U.S.C. § 9013(c).

19. See Intelligence Reform and Terrorism Prevention Act 2004, 50 U.S.C. § 403-3d; Pub. L. 108-458; 188 Stat. 3688.

20. Headquarters Air Force (HAF) Mission Directive 1-33, *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance, and Reconnaissance*, para. 3.12.

21. Air Force Instruction (AFI) 71-101V4, *Counterintelligence,* para. 1.

22. Air Force Manual (AFMAN) 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, paras. 2.5.2, 2.5.5. See also Department of the Air Force, Program Guidance Letter (PGL 19-05), *Establishment of the Information Warfare (IW) Component*.

23. Office of the Director of National Intelligence, *Intelligence Community Legal Reference Book*.

24. EO 12333, United States Intelligence Activities, Sec. 1.10(a)-(c).

25. EO 12333, Sec. 1.10(k).

26. See, for example, Department of the Air Force, 2018 CJCS Defense Support of Civil Authorities EXORD, para. 3.L.6.

27. See Office of the Director of National Intelligence, "Members of the IC [Intelligence Community]."

28. Department of Defense Directive (DODD) 5105.21, *Defense Intelligence Agency*, para. 4.

29. DODD 5105.21, para. 4.2.

30. DODD 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, paras. 6.a.(1)-(12).

31. See EO 12333, United States Intelligence Activities, Sec. 1.3(b)(12)(A)(i); and DODD 5100.20, para. 8.b.(g), respectively.

32. U.S. Const. art. 1, § 8.

33. U.S. Const. art. 1, § 8.

34. 50 U.S.C. § 3091.

35. National Security Act of 1947 (50 U.S.C. § 3091 [1991]), sec. 501.

36. 50 U.S.C. § 3093, sec. 503.

37. Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 539–629.

38. Wall, "Demystifying the Title 10–Title 50 Debate," 85.

39. Berger, "Covert Action: Title 10, Title 50, and the Chain of Command," 32–39.

40. DODD 5240.01, *DoD Intelligence Activities*.

41. See DODM 5240.01, *Conduct of DoD Intelligence,* Glossary.

42. DOD 5240.01-R, *Procedures Governing the Activities of DoD Intelligence Components.*

43. DODD 5148.13, *Intelligence Oversight*.

44. DODM 5240.01, *Conduct of DoD Intelligence,* para. 3.5.f.

45. DODM 5240.01, paras. 3.2.c., 3.2.d., and 3.2.g., respectively.

46. DODM 5240.01, para. 3.3.c.

47. DODM 5240.01, para. 3.2.f.(3). For additional information on PAI, see DODD 3115.18, *DoD Access to and Use of PAI*.

48. DODM 5240.01, para. 3.1.b.(2).

49. DODD 3115.18, *DoD Access to and Use of Publicly Available Information*, para. 1.2.b. See also AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*.

50. DODD 3115.18, para. 1.2.b.(1).

51. DODD 3115.18, para. 1.2.b.(2).

52. DODD 3115.18, Glossary, 12; and DODM 5240.01, *Conduct of DoD Intelligence*, Glossary.

53. EO 12333, United States Intelligence Activities, Sec. 3.5(h)(8).

54. EO 12333, Sec. 3.5(g).

55. EO 12333, Sec. 1.7.(f).

56. AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, paras. 2.5.1., 2.5.2.

57. Air Combat Command Manual (ACCMAN) 14-402, *Unit-Level Intelligence Mission and Responsibilities*, para. 1.2.

58. See ACCMAN 14-402, chap. 6.

59. See, for example, AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, paras. 3.4-3.4.2 (authorizing the Air Force intelligence element to collect PAI and produce open-source intelligence from it).

60. See DODM 5240.01, *Conduct of DoD Intelligence*, para. 3.2.d (permitting the temporary retention of voluntarily provided data so that it can be analyzed for permanent retention and possibly disseminated as intelligence products).

Chapter 4

DOD Cyberspace Organizations

I. Legal Authorities for Operational Cyberspace Organizations

The Department of the Air Force, pursuant to 10 U.S.C. § 9013, is responsible for organizing, training, and equipping its cyberspace operations forces. U.S. Cyber Command (USCYBERCOM) is a unified combatant command (CCMD), with CCMD authorities under 10 U.S.C. §§ 161-167(b) to employ assigned forces to perform missions assigned by the President. In the Unified Command Plan (UCP), the President has assigned USCYBERCOM the responsibilities of planning and executing global cyberspace operations. In Global Force Management Implementation Guidance (GFMIG), the Secretary of Defense (SecDef) has directed the Secretary of the Air Force (SECAF) to assign particular Air Force cyber forces to USCYBERCOM.

A. Goldwater-Nichols Act

1. The Goldwater-Nichols Department of Defense (DOD) Reorganization Act of 1986 was the largest shake-up of the DOD since the National Security Act of 1947, which merged the Department of War with the Department of the Navy and established the U.S. Air Force as an independent branch of the armed forces.[1] Congress passed Goldwater-Nichols with the goal of "enhance[ing] the effectiveness of military operations and improv[ing] the management and administration of the Department of Defense."[2] A major impetus for the act's passage was several failed joint operations, including an attempted rescue mission during the Iran hostage crisis and perceived missteps during the Grenada invasion.[3]

2. Goldwater-Nichols gave the Chairman of the Joint Chiefs of Staffs (CJCS) control over joint doctrine. It made the CJCS the primary adviser to the President, National Security Council (NSC), and SecDef, as opposed to the Service chiefs.[4] Goldwater-Nichols also clarified that unified combatant commanders (or combatant commanders) (CCDR) would report directly to SecDef but authorized the CJCS to be the SecDef's primary communication channel, which has been the standard practice.[5] Goldwater-Nichols also expanded the CCDR's authority and responsibility, *assigning* forces

under the Services' jurisdiction to a combatant command.[6] After Goldwater-Nichols, the Services generally only retain forces to perform the Military Department's mission (e.g., organize, train, and equip) or missions not directly tied to an immediate operational objective (e.g., recruiting).[7]

3. The CCMDs are organized based either on geography (e.g., Southern Command [USSOUTHCOM]) or function (e.g., Transportation Command [USTRANSCOM]).[8] Forces may only be transferred to different CCMDs prescribed by the Secretary of Defense and approved by the President.[9]

4. In 2010, CYBERCOM was designated a subunified command under U.S. Strategic Command (USSTRATCOM). USCYBERCOM was elevated to a unified combatant command on May 4, 2018, giving the Commander, USCYBERCOM (CDRUSCYBERCOM), direct reporting authority to the SecDef.[10] USCYBERCOM is the nation's 10th unified combatant command.[11]

5. CDRUSCYBERCOM commands a preponderance of cyberspace forces not retained by the Services.[12] Many of these cyberspace forces remain at their home stations (as GFMIG assigned to USCYBERCOM), the equivalent of being deployed in place. Thus, transferring them to a different CCMD would require SecDef approval. The GFMIG process is explained in section II (p. 58).

B. U.S. Cyber Command

1. USCYBERCOM is a unified combatant command charged with defending the nation in cyberspace. It has two primary missions: (1) securing, operating, and defending the Department of Defense Information Network (DODIN) and (2) engaging strategic threats in cyberspace, both directly and by supporting the military operations of geographic combatant commanders in and through cyberspace.

2. USCYBERCOM's missions were once dispersed among myriad DOD organizations, including the DOD chief information officer (CIO), Defense Information Systems Agency (DISA), the military Services, and Defense Intelligence Components. These organizations retain an important and distinct role in cyberspace. However, USCYBERCOM has a key coordinating function for military cyberspace operations to maintain strategic harmony among the DOD entities operating in this domain. Understanding the role of

USCYBERCOM in protecting the nation in cyberspace requires an awareness of the evolution of DOD organizations that eventually led to the creation of USCYBERCOM and its elevation to a unified combatant command.[13]

3. USCYBERCOM also supports and coordinates operations with other federal agencies accomplishing integral functions in cyberspace, such as the Department of Homeland Security and the Department of Justice. Cyberspace's unique characteristics make interagency coordination and deconfliction essential to the conduct of military cyberspace operations. These include the difficulty of drawing geographically or functionally distinct areas of operations in cyberspace and the growing convergence of various forms of human activity onto Internet-based technology,

4. Unless otherwise directed by the SecDef, all active and reserve cyber operations forces of the armed forces stationed in the United States shall be assigned to USCYBERCOM (10 U.S.C. 167b).

C. Commander, USCYBERCOM. CDRUSCYBERCOM is currently dual-hatted as the director of the National Security Agency (NSA)—a member of the intelligence community and a DOD combat support agency. Although not required, this arrangement reflects the vital partnership between military cyberspace operations and the national intelligence community's activities.

1. It should be noted that the NSA has overall control and direction of signals intelligence (SIGINT) collection, to include collection by cyber means, in the United States.[14]

2. Additionally, and most significantly for Air Force judge advocates advising local commanders, the borderless nature of cyberspace highlights why "local" matters in their installation's networks could have an unintended strategic impact. It also shows why consulting Air Force commands responsible for cyberspace operations is essential.

D. Joint Force Headquarters – Cyberspace, Air Force (JFHQ-C [AF]) is a component of USCYBERCOM with operational control (OPCON) of assigned joint forces (such as combat mission teams [CMT] and cyber support teams [CST]). Its mission is to provide general support—as defined by the *Doctrine for the Armed Forces of the United States*—for offensive cyberspace operations (OCO) to the United States Euro-

pean, Strategic, Transportation, and Space Commands.[15] For further information on CMTs, CSTs, and related elements of the Cyber Mission Force (CMF), reference USCYBERCOM's 2018 press release.[16]

E. Air Forces Cyber (AFCYBER). AFCYBER is the Service cyberspace component of USCYBERCOM and exercises OPCON over assigned forces (such as cyberspace protection teams [CPT]). AFCYBER's mission is executing DODIN ops and conducting defensive cyberspace ops on the Air Force Information Network. The AFCYBER commander is also the commander of Air Force forces presented to USCYBERCOM. The USCYBERCOM commander has delegated directive authority for cyberspace operations (DACO) to the AFCYBER commander, through the Joint Force Headquarters – Department of Defense Information Network (JFHQ-DODIN) commander, to exercise DACO over Air Force forces operating on the AFIN.

F. Commander, Sixteenth Air Force (16 AF). The 16 AF commander has five roles or "hats." These roles include 16 AF/CC, Defense Intelligence Component Head (AF); Service Cyberspace Component commander (CDRAFCYBER); Commander, Joint Force Headquarters – Cyberspace (CDRJFHQ-C [AF]); and the Head, Service Cryptologic Component (AF). Of the five roles, two components (AFCYBER and JFHQ-C [AF]) are OPCON to the CDRUSCYBERCOM.

G. Commander, Air Combat Command (ACC). ACC/CC is responsible for organizing, training, and equipping assigned cyber forces and provisioning the Air Force Network (AFNET) and Air Force Network – Secure (AFNET-S) for operations.

   1. On February 8, 2018, the Air Force transferred lead command for cyberspace from Air Force Space Command to Air Combat Command.[17]

   2. A lead command is a major command (MAJCOM) the Secretary has authorized to promulgate guidance across traditional organizational lines (i.e., for other MAJCOMs) for specific Headquarters Air Force–designated mission areas, weapon systems, or activities.[18]

H. Commander, 67th Cyberspace Wing (67 CW). The 67 CW commander is responsible for executing the Service mission of organizing, training, and equipping the Cyber Mission Force. The 67 CW serves as the execution arm for generating, projecting, and sustaining combat power with the employment of the Cyberspace Vulnerability

Assessment/Hunter (CVA/H) weapon system. Its Airmen conduct network operations, defense, attack, and exploitation in service of the Air Force, combatant commands, and national agencies. The 67 CW is also a designated federal laboratory, authorizing the 67 CW commander to engage industry partners in cooperative research and development agreements (CRADA) and license Air Force–developed software.

I. Commander, 688th Cyberspace Wing (688 CW). The 688 CW commander is responsible for engineering, building, operating, securing, defending, and extending the Air Force cyberspace domain. The 688 CW is also a designated federal laboratory, authorizing the 688 CW commander to engage industry partners in CRADAs.

J. 616th Operations Center (OC). The 616 OC serves two primary and distinct functions: coordination of intelligence, surveillance, and reconnaissance activities by Service-retained intelligence forces and command and control (C2) of cyberspace forces assigned to AFCYBER and JFHQ-C (AF). It also issues cyber orders as directed by CDRAFCYBER to Air Force units operating on the AFIN. For OCOs, the 616 OC publishes the cyber tasking order (CTO) under CDRJFHQ-C (AF) authority and maintains oversight of scheduled offensive missions.

K. Joint Force Headquarters – Department of Defense Information Network. JFHQ-DODIN is a component command of USCYBERCOM and functions at the operational level of warfare to secure, operate, and defend DODIN infrastructure and networks worldwide. To ensure unity of effort, it exercises tactical control (TACON) over all DOD components that conduct DODIN and defensive cyberspace operations–internal defensive measures (DCO-IDM) operations to defeat, deny, and disrupt cyberattacks against the DODIN. This includes TACON over Service cyberspace components, such as Air Forces Cyber. JFHQ-DODIN also serves as a supporting command for regional and component commands by conducting DODIN and DCO-IDM operations to augment the supported component's warfighting functions. The JFHQ-DODIN commander also serves as the DISA director.

L. Defense Information Systems Agency (DISA). DISA is a combat support agency of the DOD. A subordinate agency to JFHQ-DODIN, DISA is tasked with executing DODIN operations and DCO-IDM at the global and enterprise levels within its portions of the DOD Information Network. However, DISA is primarily responsible for provid-

ing information technology infrastructure for the DOD and, to secure that technology, also provides resources and implements unified standards. Through its infrastructure directorate, DISA implements and secures the DODIN's core infrastructure and capabilities for all DODIN components—including the AFIN. As part of this mission, DISA is critical to securing the DODIN infrastructure and monitors and evaluates data routed throughout the entire DODIN, allowing it to maintain situational awareness of all threats and reduce threat response times.

II. Categories of Forces and Global Force Management

A. Categories of Forces

1. Goldwater-Nichols divides military forces into two broad categories. In the first category are forces presented to the SecDef by the Services for assignment to CCMDs or the United States element of the North American Aerospace Defense Command (NORAD).[19] These are the forces that conduct military operations.[20] In the second category are forces that remain assigned to the Services to execute Secretarial responsibilities.[21] For purposes of this discussion, Secretarial responsibilities generally consist of preparing and training forces to conduct military operations in support of a CCDR and sustaining and supporting those already so employed.[22]

2. The second category, assignment of forces to the Services, is the DOD default position, so no special process is necessary to accomplish it. For example, Air Force forces remain assigned to the Air Force unless affirmatively presented to the SecDef and assigned elsewhere. Forces assigned to CCMDs, on the other hand, require special processing to invoke that assignment. This process is known as global force management (GFM).

B. Global Force Management

1. GFM is the process by which the SecDef manages the employment of force by CCDRs.[23] The process is rooted in the Unified Command Plan (UCP) in which the President "sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders."[24] The Defense Strategy Review, joint

force availability requirements, and joint force assessments inform the execution of the UCP. Through these resources, the SecDef determines how forces should be assigned, allocated, and apportioned among the various CCMDs.

2. *Assignment* in the context of GFM is the process by which a Service Secretary assigns military forces to CCMDs when directed to do so by the SecDef.[25] The SecDef communicates this direction through the Global Force Management Implementation Guidance document.[26] *Allocation* is the process by which the SecDef temporarily adjusts the distribution of forces among the CCDRs.[27] For example, a unit assigned to one CCDR can be allocated to another CCDR for a specific mission or operational need. *Temporarily adjusts* is a relative term in the allocation context, as allocation of forces also encompasses rotational requirements like the Air Expeditionary Force deployment cycle.[28] The SecDef communicates allocation decisions in the Chairman of the Joint Chiefs of Staff (CJCS) annual deployment order, more commonly referred to as the Global Force Management Allocation Plan (GFMAP).[29] *Apportionment* is an estimate of forces and resources the Services are expected to be able to generate for CCMD employment during a given year.[30] This estimate is used as a planning tool for future force employment.

3. Assignment of forces is the most critical GFM process for this discussion, as it is how cyber mission forces are placed under the authority of U.S. Cyber Command.[31] As mentioned, the GFMIG is the document through which the SecDef communicates CCMD assignments. Additionally, within the GFMIG are allocation tables through which the SecDef assigns forces by levying specific requirements on each Service.[32] These force requirements are typically expressed in terms of capabilities, and it is the Service Secretaries who identify the units that will meet the capability requirement.[33] Once identified, these units become assigned to the CCMD to which they have been directed, and the CCDR exercises combatant command authority (COCOM) over them.[34] Air Force Instruction (AFI) 10-401 describes the process by which the SECAF identifies units and Airmen meeting GFMIG requirements, including those assigned to USCYBERCOM.[35]

4. The GFMIG assignment process described above is relatively straightforward in concept but can be complex in application from a legal practitioner's perspective. For instance, the Service cyberspace components, which include AFCYBER, are assigned to USCYBERCOM and are under the COCOM of its commander.[36] AFCYBER comprises Air Force and joint personnel, and while Air Force units use the familiar squadron-group-wing nomenclature, those units also supply personnel for the joint teams that compose various parts of the Cyber Mission Force. The result is that units and personnel with every appearance of being in the Air Force may only be so for administrative purposes. Air Force intelligence forces assigned to USCYBERCOM can further complicate matters. For example, part of an intelligence unit could be GFMIG-assigned to USCYBERCOM while other parts of the unit are Service-retained and operate under the authority of a different chain of command. The separation of unit members adds a layer of complexity to operations because personnel in the same unit may be subject to different legal and policy regimes and may not be authorized to conduct the same operations.

5. Many cyberspace and intelligence professionals are unaware of these nuances. Legal practitioners must be prepared to articulate why Airman A can occupy a particular position and perform certain functions, but Airman B cannot. Further, practitioners should be able to discuss why Air Force policy applies to certain unit activities while USCYBERCOM policies and requirements apply to others. Practitioners must fully educate themselves on these nuances because misstating authorities or details could lead to questionable intelligence activities and cyberspace operations that lack or exceed authority. Accordingly, attorneys must have a working knowledge of the GFM process and specific knowledge of which personnel are GFMIG assigned in units they support. For further information, contact ACC/JA or 16 AF/JA.

III. Cyberspace Operations Forces

USCYBERCOM and other CCMDs have designated cyberspace operations forces to plan and execute cyberspace operations.

A. Combatant Command Cyberspace Operations Support Staffs. CCDRs tailor their respective staffs to their mission. For cyberspace operations, a CYBERCOM Cyberspace Operations – Integrated

Planning Element (CO-IPE) is incorporated into each CCMD staff. The CO-IPE is tailored to the supported CCMD. CO-IPEs provide CCDRs with cyberspace operations planners and other subject matter experts required to support the development of CCMD requirements for cyberspace ops and to assist CCMD planners with coordinating, integrating, and deconflicting these operations.

B. Mission-Tailored Force Package (MTFP). A MTFP is a CYBERCOM-tailored support capability comprised of assigned cyberspace operations forces, additional cyberspace operations support personnel, and cyberspace capabilities as required. When directed, CYBERCOM establishes MTFPs to support specific CCMD crisis or contingency mission requirements beyond the capacity of forces available for routine support. A MTFP will typically dissolve once the contingency is complete.

C. Joint Force Headquarters – Department of Defense Information Network. JFHQ-DODIN is responsible for the operational-level planning, direction, coordination, execution, and oversight of global DOD Information Network operations and DCO-IDM missions. It maintains support relationships, as established by CDRUSCYBERCOM, with all CCDRs for theater/functional DODIN operations and DCO-IDM. The JFHQ-DODIN commander is supported for global DODIN operations and DCO-IDM. Combatant commanders are supported for DODIN operations and DCO-IDM with effects contained within their AOR or functional mission area. The JFHQ-DODIN commander exercises directive authority for cyberspace ops over all Department of Defense components as delegated by CDRUSCYBERCOM.[37]

D. Cyber Mission Force (CMF). USCYBERCOM's Cyber Mission Force supports the DOD Cyber Strategy through the three subteams detailed below.

1. In 2012, the SecDef and CJCS established the CMF to organize and resource the force structure required to conduct key cyberspace missions.[38] Essentially, the task was to create a skilled cyber workforce to implement the DOD's three primary cyber missions by training and equipping CMF teams. By 2018, all 133 CMF teams were fully operational and included all Services (Army, Air Force, Navy, and Marines) as well as National Guard and reserve personnel, comprising over 6,200 individuals.[39]

2. The focus has shifted to maintaining a trained CMF, which is congressionally mandated to certify operational capacity every two years.[40] Training is primarily accomplished through four phases, with the individual Services conducting Phase 1. Later phases of training have standards set by USCYBERCOM and training administered by the Services collectively, by USCYBERCOM or the NSA, or at the unit level (depending on training phase).[41] In late 2020, the 67th Cyberspace Wing stood up a new group, the 867th Cyber Operations Group, to bring all Air Force Cyber Mission Force teams under the same ADCON.
3. Cyber Protection Force (CPF). The first of the three sub-teams, the CPF conducts cyberspace operations for internal protection of the DODIN and other Blue Cyberspace when ordered. CPFs are composed of cyberspace protection teams (39-person "threat-specific" teams allocated to an operational command [i.e., USCYBERCOM]) and aligned along four mission areas: CCMD support, Service reallocated (i.e., USAF, USN), DODIN ops, or national threat response. Organized, trained, and equipped by the Services, CPTs typically perform survey, protect, and secure missions. Combatant command CPTs are OPCON to the CCDR to which they are aligned and provide DCO support to the network or DODIN enclave specific to that CCMD.
4. Cyber National Mission Force (CNMF). The second sub-team, the CNMF conducts cyberspace operations to defeat significant cyberspace threats to the DODIN and, when ordered, to the nation. The CNMF comprises various numbered national mission teams (NMT), associated national support teams (NST), and national-level CPTs for the protection of non-DODIN Blue Cyberspace. CNMF teams engage in hunt-forward operations and are tasked with pursuing high-priority targets identified by SecDef and CDRUSCYBERCOM.[42]

    a) National Mission Teams (NMT). NMTs are tactical units of the CNMF that defend the DODIN or other Blue Cyberspace when ordered, to include defensive cyberspace operations–response actions (DCO-RA) missions. The NMTs are aligned under the CNMF-HQ against specific cyberspace threats. NMTs conduct offensive cyberspace operations missions similar to those assigned to CMTs but not necessarily in direct support of CCDR objectives. They typically focus on plans and priorities to proj-

ect power in support of national objectives and defend forward on non-DOD cyberspace with the permission of allies and mission partners.

b) National Support Teams (NST). NSTs are technical teams that provide specialized technical and analytic support for the NMTs. This support can include intelligence analysis, cyberspace capability development, linguist support, and planning.

5. Cyber Combat Mission Force (CCMF). The CCMF, the third subteam, conducts cyberspace operations to support the missions, plans, and priorities of the geographic and functional CCDRs. The CCMF comprises various numbered combat mission teams (CMT) and associated combat support teams (see fig. 4.1).

   a) Combat Mission Teams (CMT). CMTs are tactical units of the CCMF, similar to NMTs. However, CMTs are aligned to provide general support to certain CCMDs based on SecDef guidance. Combat mission teams typically support the plans and objectives of the combatant commander with whom they are aligned. Notably, these CMTs are not under the combatant commander's OPCON but work through CO-IPEs in the combatant command staff to synchronize and align CCDR intent and guidance.

   b) Cyber Support Teams (CST). CSTs are similar to NSTs but support the CMT(s) they are aligned with.

E. Joint Force Headquarters – Cyberspace (JFHQ-C). The Secretary of Defense aligned the offensive portion of cyber mission forces into JFHQ-Cs that fall under the USCYBERCOM commander. JFHQ-Cs have OPCON over the CMTs that conduct offensive cyberspace operations. Each JFHQ-C is under the OPCON of USCYBERCOM but aligned to provide general support for OCOs to the specific or CCMDs shown below (see figs. 4.1 and 4.2 and table 4.1).

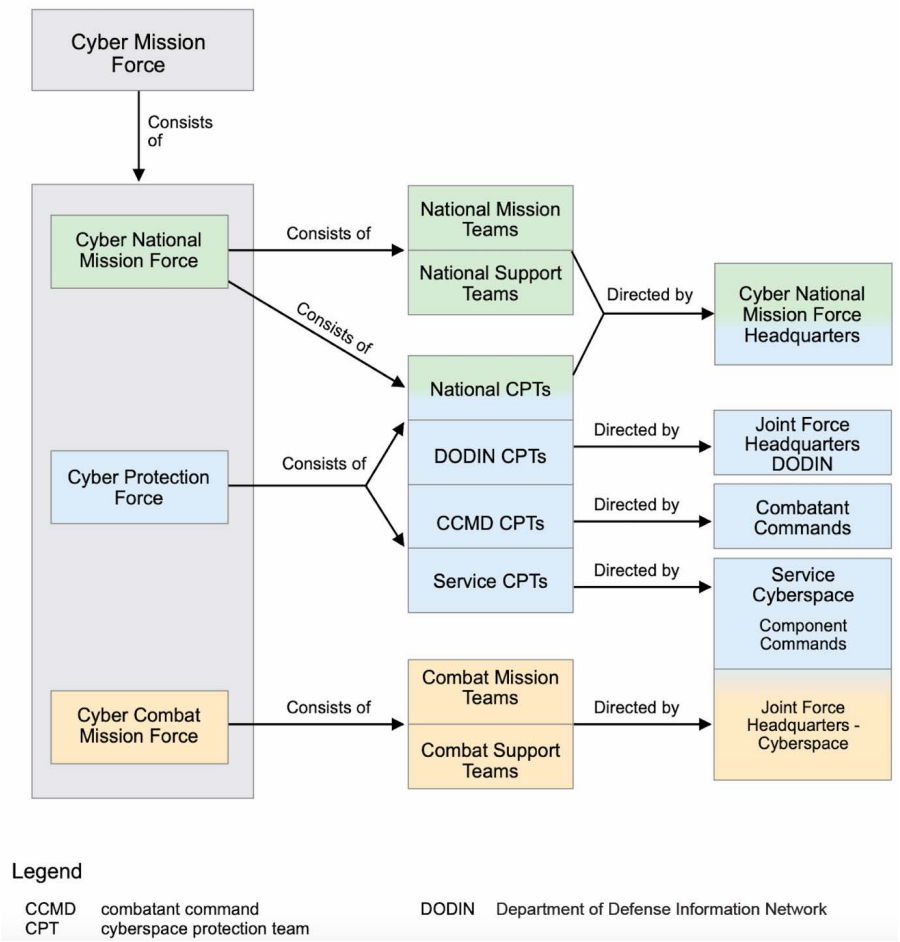


Figure 4.1. DOD Cyber Mission Force relationships. (JP 3-12, *Cyberspace Operations*, June 8, 2018, fig. I-2, I-10, https://www.jcs.mil/.)

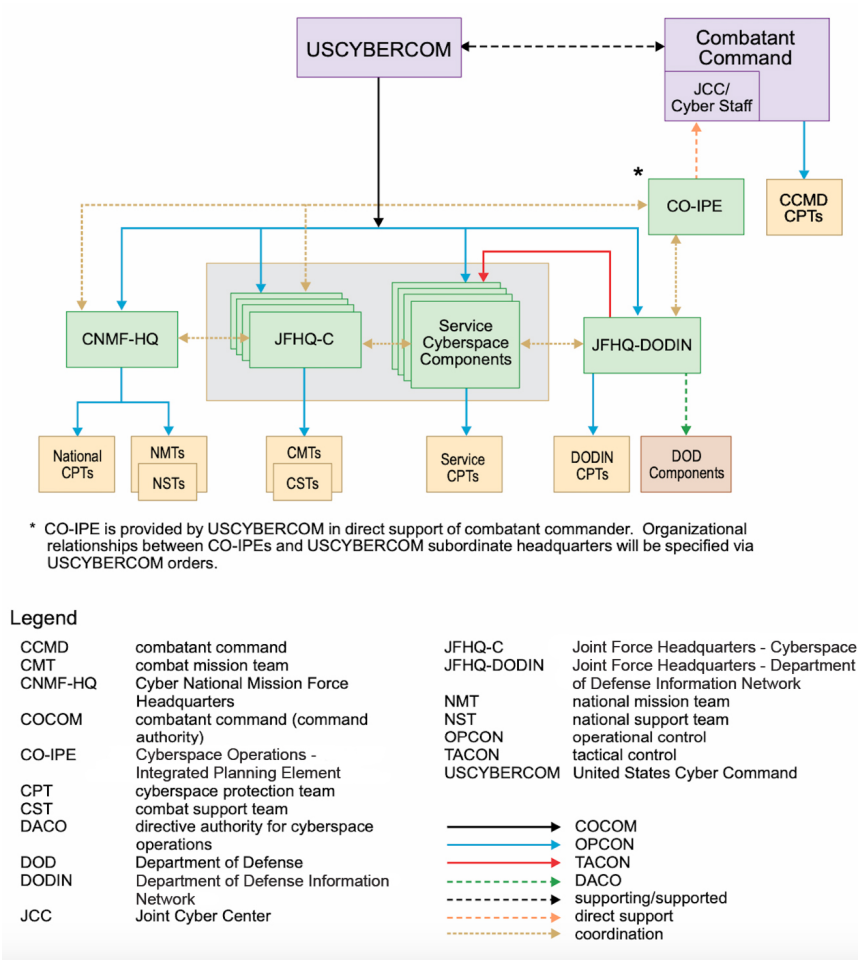


Figure 4.2. Routine cyberspace command and control. (JP 3-12, *Cyberspace Operations*, June 8, 2018, fig. IV-1, IV-13, https://www.jcs.mil/.)

Table 4.1. Service division of responsibilities

Service Component	Area of Responsibility
JFHQ-C (Marines)	U.S. Special Operations Command (SOCOM)
JFHQ-C (Army)	U.S. Central Command (CENTCOM) U.S. Africa Command (AFRICOM) U.S. Northern Command (NORTHCOM)
JFHQ-C (Navy)	U.S. Pacific Command (PACOM) U.S. Southern Command (SOUTHCOM)
JFHQ-C (Air Force)	U.S. European Command (EUCOM) U.S. Strategic Command (STRATCOM) U.S. Transportation Command (TRANSCOM) U.S. Space Command (SPACECOM)

IV. Cyberspace Operations Missions

A. DODIN operations are intended to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the DOD Information Network (see table 4.2).

Table 4.2. Cyberspace operations missions

	Cyber Ops Mission				
	OT&E	**DODIN Ops**	**DCO-IDM**	**DCO-RA**	**OCO**
Description	Design & build	Threat-agnostic ops & security	Internal response to specific threat	External response to specific threat	External power projection
CO Actions	N/A	Security	Defense	Exploitation Attack (D4M)	Collect/ Exploit/ Attack
Cyber Terrain	Blue (consent)	Blue (consent)	Blue (consent)	Gray & Red	Gray & Red
Authority Line	Service	CCMD	CCMD	CCMD	CCMD
LoW/ROE (law of war / rules of engagement)	N/A	N/A	N/A	Applies	Applies
Forces	Service	Service & CPF	CPF	CMF (CNMF)	CMF

B. Defensive cyberspace operations (DCO) missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace.

C. Offensive cyberspace operations are missions intended to project power in and through foreign cyberspace through actions taken in support of the CCDR or national objectives. OCOs include everything from collection to deny, degrade, disrupt, destroy, or manipulate (D4M) effects.

V. Mission Defense Teams

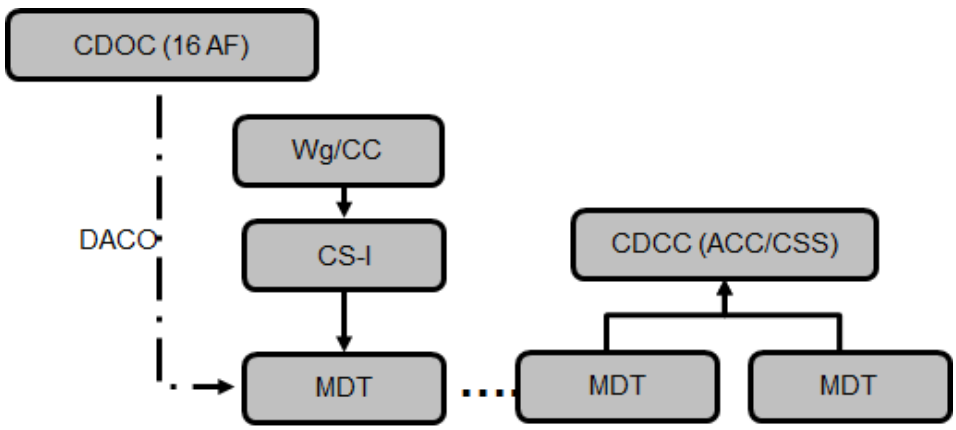
A. Mission defense teams (MDT) are "Service-retained" forces under 10 U.S.C. § 9013. This is important because the wing "owns" these forces, much like a base security forces squadron or mission support group. DOD cyberspace operations forces (COF), active and reserve, are assigned to USCYBERCOM under 10 U.S.C. § 167b through the global force management process discussed above. Forces not assigned to USCYBERCOM via the GFM process remain either assigned to another combatant command or are Service retained. DOD COFs consist of "units organized, trained, and equipped to conduct offensive cyberspace . . . , defensive cyberspace . . . , and Department of Defense Information Network . . . operations." A 2019 SecDef memorandum explicitly categorizes MDTs as Service-retained forces, thereby excluding MDTs from the DOD COF.[43]

B. MDTs are an outgrowth of the Cyber Squadron Initiative (CS-I). The CS-I intends to repurpose and reorganize base-level communications squadrons into cyber squadrons with the mission to protect "Air Force core missions from threats in, . . . [through], and from cyberspace."[44] Consequently, MDTs are a mission-assurance force intended to exist within the Air Force's organize, train, and equip (OT&E) mission, but they could be capable of supporting ongoing military operations much the same as would any steady-state subordinate squadron under a wing. Their authorities and command and control are no different than the standard Service-retained communications squadrons that preceded them.

1. Though the commander, Sixteenth Air Force (AFCYBER), does not exercise OPCON over MDTs, their role as CDRAFCYBER allows them to issue orders under their directive authority to conduct cyberspace operations via the 616 OC. DACO is the authority

to issue orders and directives for executing DODIN operations and defensive cyberspace operations–internal defensive measures to compel unity of action to secure, operate, and defend the DODIN. AFCYBER does not generally issue orders directly to MDTs. DACO is explained at greater length below.

2. The Cyber Defense Coordination Center (CDCC) is a mid-tier organization located at the MAJCOM level to coordinate actions between individual wing MDTs to ensure unity of effort. CDCCs are not intended to override the wing's C2 of its forces. Instead, they are designed to coordinate and support the efforts of MDTs in defending their systems (fig. 4.3).



Legend

CDOC Cyberspace Defense Operations Center
CSS Communications Support Squadron

Figure 4.3. Mission defense team concept

C. MDTs are typically assigned to secure a weapon system. They are tasked to provide wing commanders with defensive measures focused on the unique wing structure and their installations' cyber infrastructure. MDTs do not conduct DODIN ops or DCO-IDM on the AFIN and do not conduct DCO-RA or OCOs in gray or red cyberspace. They are limited to operations within their installation's boundary. The CDRAFCYBER, through 16 AF/CC, can mandate particular security-related actions under the directive authority for cyberspace operations.

1. DACO is the authority to issue orders and directives to all DOD components directing the execution of global DODIN operations and DCO-IDM to compel unity of action to secure, operate, and defend the DODIN.[45] Per the CJCS C2 Execute Order (EXORD) for Cyberspace, DACO is vested in CDRUSCYBERCOM.[46] CDRUSCYBERCOM can transfer or delegate DACO in total, or for specific times and purposes, to ensure the timely and efficient operation and defense of the DODIN.

2. CDRUSCYBERCOM has delegated DACO to JFHQ-DODIN covering all DOD components that conduct DODIN operations and DCO-IDM on the DODIN that is not under the DACO authority of Service cyberspace components or other designated commanders. CDRUSCYBERCOM also delegated DACO to all Service cyberspace components over their respective Service DOD components that conduct DODIN operations and DCO-IDM on the DODIN. Consequently, CDRAFCYBER may order any Air Force command, unit, or entity—whether or not it belongs to AFCYBER—to take actions to ensure the security, operation, and defense of the AFIN.

D. Mission Assurance Authorities. The authority under which MDTs operate are referred to in the cyber community as chief information officer or CIO authorities under Titles 40 and 44 U.S.C. for network security, mission assurance, and network defense. CIO authority is merely a term of art used to describe the statutory responsibilities common to all Service-level CIOs.

   1. Communications and information security authority derive statutorily from the Federal Information Security Modernization Act of 2014 (FISMA 2014).[47] FISMA 2014 amended FISMA 2002, which fell under Title III of the overarching E-Government Act.[48] FISMA 2002, as amended, established the National Institute of Standards and Technology (NIST) as the agency responsible for promulgating computer security standards for all federal agencies. The act also mandated that federal agencies annually develop and document information security compliance for their respective information systems. Further, they were required to have annual certification and reports for information awareness training. The Department of the Air Force requires annual information awareness training for access to its information system or network.

a) The FISMA 2014's amendments made beneficial modifications to the law. They included fewer cumbersome reporting requirements, less impositions on agencies for the use of continuous monitoring on their systems, and reduced reliance on the agency for compliance. Also, reporting focused on security incidents versus overarching quarterly standard reports to increase incident information crossflow between agencies. Agency-led continuous monitoring on information systems is typically accomplished by Air Force units using unclassified cyber defense weapon systems such as CVA/H and other weapon systems.[49]

b) A critical item required not only by FISMA 2014 but also by the Paperwork Reduction Act of 1995 44 U.S.C. § 3501 *et seq.*, Pub. L. 104-13, 109-435, 110-289, and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), 40 U.S.C. Subtitle III, Pub. L. 104-106, frames authority from the perspective of security protocols focused on balancing risk versus costs. Ostensibly, the law intends to empower "responsible officials"—typically CIOs and their designees—to oversee their entire network security program and make investment judgments that provide "adequate security" to mitigate risk to their systems. Such a security risk calculus is intended to factor consequences like the magnitude of harm likely to result from unauthorized access, destruction, disruption, disclosure, or modification of information on the network. It is also important to note that under 44 U.S.C. § 3544(a)(1)(B), the FISMA 2014 directs all agencies to comply with security protocols, policy, and standards promulgated by the NIST. For NIST authority to disburse policy for the U.S. Government, see 40 U.S.C. § 11331.

c) The DOD has promulgated several authoritative documents that expand upon the various Service CIO authorities to defend their respective information networks and national security systems.[50] FISMA 2014 defines a *national security system* (NSS) as "any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency."[51] Readers will likely note the definition of NSS as ostensibly mirroring other definitions of *network* throughout this guide.

d) Other key authoritative guidance may be found in DOD Directive 3020.40, *Mission Assurance*. This directive authorizes CIOs and their respective designees to "protect or ensure the continued function and resilience of capabilities and assets."[52] These authorities are carried forward in the Air Force via AFI 17-130, *Cybersecurity Program Management*, February 13, 2020, and AFMAN 17-1301, *Computer Security (COMPUSEC)*, February 12, 2020.[53] Both documents provide detailed guidance on how the Air Force secures the network.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433, 100 Stat. 992 (1986) [hereinafter Goldwater-Nichols]. See National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 (1947).
2. Goldwater-Nichols § 3(8).
3. See Kitfield, "*Better Way to Run a War.*"
4. See International and Operational Law Department, Judge Advocate General's Legal Center and School, U.S. Army, *Operational Law Handbook.*
5. See International and Operational Law Department, *Operational Law Handbook.*
6. International and Operational Law Department, 443.
7. Department of the Air Force Instruction (DAFI) 10-401, *Air Force Operations Planning and Execution*; see also Judge Advocate General's School, *Law of Air, Space, and Cyber Operations*, 166.
8. Judge Advocate General's School, *Law of Air, Space, and Cyber Operations*, 168.
9. See 10 U.S.C. § 162.
10. U.S. Cyber Command, "Our History."
11. U.S. Cyber Command, "Our History."
12. Joint Publication (JP) 3-12, *Cyberspace Operations*, I-8, para. 4.a.
13. See U.S. Cyber Command, "Our History."
14. See DOD Directive 5100.20*, National Security Agency/Central Security Service.*
15. JP 1, *Doctrine for the Armed Forces of the United States.*
16. U.S. Cyber Command, "Cyber Mission Force Achieves Full Operational Capability."
17. Headquarters Air Force, Program Guidance Letter (PGL) L18-22, *Transfer of cyberspace lead command.* See also DAFPD 17-2, *Cyber Warfare Operations*, para. 3.7.
18. Department of the Air Force Instruction (DAFI) 33-360, *Publications and Forms Management*, para. 1.2.3.2.
19. 10 U.S.C. § 162(a)(1).
20. 10 U.S.C. § 162(a)(1).

21. 10 U.S.C. § 162(a)(2).

22. See 10 U.S.C. §§ 7013; see also JP 1, *Doctrine for the Armed Forces of the United States*, II-11–II-12 (discussing the role of Services in the DOD's joint operational construct).

23. JP 3-35, *Deployment and Redeployment Operations*, I-4.

24. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Term*s, 224.

25. JP 3-35, *Deployment and Redeployment Operations*, I-4.

26. JP 3-35, I-4.

27. JP 3-35, I-4.

28. *CJCS Guide* 3130, *Adaptive Planning and Execution Overview and Policy Framework,* GL-3.

29. JP 3-35, *Deployment and Redeployment Operations,* I-4.

30. JP 3-35, I-5; see also CJCS Guide 3130, *Adaptive Planning and Execution,* GL-3.

31. 10 U.S.C. § 167b(b).

32. JP 3-35, *Deployment and Redeployment Operations,* I-4.

33. JP 3-35, I-4; and 10 U.S.C. § 9013(g)(1).

34. JP 3-35, I-4.

35. DAFI 10-401, *Air Force Operations Planning and Execution.*

36. See 10 U.S.C. § 167b(b); see also JP 3-12, *Cyberspace Operations*, fig. IV-1.

37. For further information on DACO, refer to sec. V, Mission Defense Teams, in this chapter.

38. JP 3-12, *Cyberspace Operations*, I-19; and U.S. Army Cyber Command, "*DoD Fact Sheet: Cyber Mission Force.*"

39. See JP 3-12, I-19; U.S. Army Cyber Command, "DoD Fact Sheet: Cyber Mission Force"; and Theohary, *Defense Primer: Cyberspace Operations*.

40. *See* Government Accountability Office (GAO), *DOD Training: U.S. Cyber Command and Services.*

41. GAO, 8-9.

42. U.S. Cyber Command, "*DOD Has Enduring Role in Election Defense.*" The article states, "An example of persistent engagement in action is 'hunt forward' operations that involve deploying defensive cyber teams around the world at the invitation of allies and partners to look for adversaries' malicious cyber activity."

43. Secretary of Defense to Chief Management Officer, Department of Defense et al., memorandum, subject: Definition of "Department of Defense Cyberspace Operations Forces."

44. Secretary of Defense, Chief Information Officer, "Cyber Squadron Enabling Concept."

45. JP 3-12, *Cyberspace Operations*, II-10.

46. MOD 001 to C2 EXORD 5.A.3.E.

47. 44 U.S.C. § 3551 *et seq.*, Pub. L. 113-283.

48. 44 U.S.C. § 3553; and 44 U.S.C. 36, *et seq.*, Pub. L. 107-347.

49. Air Combat Command Manual 17-2CVA/H, vol. 3, *Cyber Vulnerability Assessment/Hunter (CVA/H) – Operations and Procedures.* See also the expanded section on cyber defense weapon systems in chap. 5, sec. 2, of this primer.

50. See DOD Instruction 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*.

51. 44 U.S.C. § 3552(b)(6)(A)(2014).

52. DOD Directive 3020.40, *Mission Assurance.*

53. See AFI 17-130, *Cybersecurity Program Management*; and AFMAN 17-1301, *Computer Security.*

Chapter 5

DOD Information Network Operations and Defensive Cyberspace Operations

I. Legal Authorities

A. The operational chain of command delegated the authority to plan, execute, direct, coordinate, and assess Department of Defense Information Network (DODIN) operations and authorized defensive cyberspace operations (DCO) to the commander, U.S. Cyber Command (CDRUSCYBERCOM), who delegated that authority (other than DCO–response actions [RA]) to Joint Force Headquarters (JFHQ)-DODIN. For the Service-specific portions of the DODIN, that responsibility is given to the Service cyberspace component commanders. For the Air Force, it means that the Air Forces Cyber commander (CDRAFCYBER) is charged with the defense and protection of the Air Force Information Network (AFIN). This authority is enabled and enforced through directive authority for cyberspace operations (DACO).

1. As noted above, in the context of mission defense teams (MDT), DACO allows CDRAFCYBER (through the 616th Operations Center [616 OC] staff) to promulgate lawful orders and directives anyone connected to the AFIN must follow. Thus, communications squadrons and units typically outside the AFCYBER chain of command must follow and incorporate updates and orders disseminated by AFCYBER (or JFHQ-DODIN) or risk having their systems disconnected from the AFIN. This authority ensures unity of action for the DODIN's timely and efficient security, operation, and defense.

2. Attorneys should note that no *operational* authority for cyberspace lies at the wing or squadron levels. The SecDef ordered all cyberspace operations to be directed through USCYBERCOM and provided no operational authority outside of the Cyber Mission Force (CMF) framework. Base-level units have responsibilities under certain JFHQ-DODIN and Service-directed policies to ensure their networks are safe, they are not connecting things that should not be connected, and they reliably manage local networks. Units must relay problems through the MAJCOM Communications Co-

ordination Center (MCCC), the Service-side hub for communications and issue resolution between local bases and AFCYBER. If attorneys receive questions at the local base level about operational missions, they should contact 16 AF/JA and confirm the authority exists or is being executed lawfully.

B. DODIN Operations. *DODIN operations* are defined as "operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network."[1] DODIN operations are network focused and threat agnostic: the cyberspace forces and workforce undertaking this mission endeavor to prevent all threats from impairing a particular network or system they are assigned to protect. DODIN operations do not include actions taken under the statutory authority of a Service chief information officer (CIO) to provision cyberspace for operations, including developing information technology (IT) architecture, establishing standards, or designing, building, or otherwise operationalizing DODIN IT for use by a commander.

C. Defensive Cyberspace Operations. JP 3-12, *Cyberspace Operations*, defines *defensive cyberspace operations* as "missions 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."[2] DCO includes two subcategories. *Defensive cyberspace operations–internal defensive measures* (DCO-IDM) are defined as "operations in which authorized defense actions occur within the defended portion of cyberspace." *Defensive cyberspace operations–response actions* (DCO-RA) are "operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system."[3]

D. Air Force Service authority to ensure cybersecurity and interoperability of Air Force networks (largely vested in the Air Force Deputy Chief Information Officer [SAF/CN]) overlaps with USCYBERCOM authority (delegated to AFCYBER) to operate, secure, and defend Air Force networks once operational. However, in addition to these delegations of authority, SAF/CN has designated 16 AF as the component cybersecurity service provider (CSSP) for the AFIN, giving

16 AF authority to ensure the AFIN is secure, assured, and interoperable and all personnel are appropriately trained.

E. Service Cyberspace Components. Service cyberspace components are separate commands that fall under the operational control (OPCON) of USCYBERCOM. They are tasked to plan, execute, direct, coordinate, and assess DODIN operations and authorized defensive cyberspace operations. Service cyberspace components exercise OPCON over cyberspace forces, including Service cyberspace protection teams (CPT), as delegated by CDRUSCYBERCOM or otherwise assigned. Service cryptologic components (SCC) also exercise administrative control over assigned forces. Each Service has a commander designated the SCC commander, dual-hatted by CDRUSCYBERCOM as commander of one of the four JFHQs-Cyber to enable synchronization of cyberspace operations command and control (C2). While the individual commander is the same, their assigned lines of authority and personnel are not. Attorneys should assist their operators and teams in understanding which line of authority gives which commander the ability to conduct a particular operation or mission and what authorities allow the command to move personnel between teams. All Service cyberspace components are OPCON to USCYBERCOM and are tactical control to JFHQ-DODIN. The Service cyberspace components are aligned as shown in table 5.1.

Table 5.1. Service cyberspace components and assigned terrain

Service Cyberspace Component	Assigned Terrain
Marine Forces Cyber Command (MARFORCYBER)	Marine Corps Enterprise Network (MCEN)
Army Cyber Command (ARCYBER)	Army Department of Defense Information Network (DODIN-A)
Fleet Cyber Command (10th Fleet/FLTCYBER)	Navy/Marine Corps Intranet (NMCI) (continental U.S. [CONUS] and outside CONUS [OCONUS]) Navy Enterprise Network (ONE-NET) (OCONUS) Next Generation Enterprise Network (NGEN) / Naval Enterprise Networks (NEN)
Air Force Cyber Command – 16 AF (AFCYBER)	Air Force Information Network (AFIN)
Coast Guard Cyber Command (COASTGUARD CYBER)	Coast Guard - Cyber

F. In the case of the Air Force, the Service cyberspace component is Air Forces Cyber (AFCYBER), and the commander is multi-hatted as commander of Sixteenth Air Force and Joint Force Headquarters – Cyberspace (JFHQ-C) (AF) (as well as the defense intelligence component and Service cryptologic component roles discussed above). The SecDef has assigned CDRAFCYBER the authority to ensure the operations, security, and defense of the Air Force portion of the DODIN (the AFIN). Accordingly, CDRAFCYBER issues cyber tasking orders (CTO) to those with systems connected to the AFIN (e.g., MAJCOMs, field commands, numbered air forces, Delta forces, wings, garrisons, integrated network operations, support centers, and communications focal points) via the 616 OC using delegated DACO (see sec. A, above). The 616 OC accomplishes this messaging and control via CTOs, maintenance tasking orders (MTO), cyber control orders (CCO), operation orders (OPORD), and tasking orders (TASKORD).

G. Defensive Tasking Processes. CPTs, 688th Cyberspace Wing (688 CW) units, and installation communication and cyber squadrons that protect Air Force networks can receive tasks through multiple channels. JFHQ-DODIN has the authority to task all Service cyberspace components to address issues affecting any DOD network via DACO. CDRAFCYBER, in their role as the Air Force Service Cyberspace Component, receives a task through the 616 OC, which then issues tasking orders to the responsible tactical unit. CPTs execute DCO missions, 688 CW units such as the Air Force Computer Emergency Response Team (AFCERT) execute AFIN operations, and installation communication squadrons or MDTs execute tasking orders for their areas of responsibility.

   1. JFHQ-DODIN can also directly task CPTs and other units to remedy vulnerabilities. When AFCYBER identifies an Air Force–specific issue, the 616 OC will task the appropriate CPT, 688 CW unit, or installation communication squadron with remediation.

   2. A similar yet distinct responsibility is that of CSSP, delegated to 16 AF/CC from the Air Force CIO.[4] This role is charged with ensuring the AFIN is secure, assured, and interoperable and all personnel are appropriately trained. Some CSSP guidance is distributed through traditional policy notification means (such as Servicewide memos or memos directly to MAJCOM/CCs). However, the 616 OC can also issue CSSP guidance.

II. Defensive Cyber Weapon Systems

A. The DOD defines a *weapon system* as a "combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."[5] Cyber capabilities are not likely to first come to mind when thinking about a weapon system. However, classifying something as a weapon system helps ensure long-term funding and sustainability. There are six primary defensive cyber weapon systems:[6]

1. Air Force Intranet Control (AFINC). The AFINC weapon system is the top-level boundary and entry point into the Air Force Information Network and controls the flow of all external and interbase traffic through standard, centrally managed gateways.[7] The AFINC integrates network operations and defense via four subdiscipline areas:

   a) Defense-in-depth: delivering an enterprise-wide layered approach integrating gateway and boundary devices to increase network resiliency and mission assurance.

   b) Proactive defense: conducting continuous monitoring of AFNET traffic for response time, throughput, and performance to ensure timely delivery of critical information.

   c) Network standardization: creating and maintaining standards and policies to protect networks, systems, and databases and reduce maintenance complexity, downtime, costs, and training requirements.

   d) Situational awareness: delivering network data flow, traffic patterns, utilization rates, and in-depth historical traffic research for anomaly resolution.

2. Cyber Defense Analysis (CDA). CDA provides operational effects designed to protect and defend critical Air Force data. It also provides monitoring and assessment of telephony, radiofrequency, email, and Internet-based capabilities and cyberspace and web operational risk assessment. CDA uses sensors to capture and assess the content of communications entering and exiting Air Force networks, focusing on preventing loss of data beneficial to adversaries. Two types of missions use CDA: electronic system security assessment (ESSA) and active indicator monitoring (AIM).[8]

a) Electronic System Security Assessment. ESSA analyzes unsecured communications to disclose sensitive information whose loss would pose a risk to operations and resources. Air Force Instruction (AFI) 10-701, *Operations Security*, outlines the purpose, authority, and limitations for the use of ESSA products.[9] An ESSA mission focuses on operations security (OPSEC) disclosures, such as flight schedules or personally identifiable information (PII). Commanders can use ESSA reports to evaluate the communication practices of their people. Release of individually attributable reports is strictly limited—the requesting commander is not provided the identity of the user who sent or received sensitive information. SECAF approval is required to use information gathered in an ESSA mission for criminal or administrative adverse actions. These policy limitations result from privacy concerns. Authority to monitor communications for ESSA missions is derived from the Federal Information Security Modernization Act, 44 U.S.C. § 3554, and implemented in AFI 10-701. ESSA missions comply with the Air Force Privacy and Civil Liberties Program, as the monitored individuals' privacy interests are balanced against the need to identify OPSEC vulnerabilities.[10]

b) Active Indicator Monitoring (AIM). CDRAFCYBER, through 616 OC, tasks CDA units to search for information vulnerabilities that would facilitate unauthorized access to the AFIN or enhance adversary cyberspace operations if intercepted by an adversary. These vulnerabilities could include usernames and passwords, network topology, or PII. AIM missions focus on the defense of the AFIN itself. Network defense is inherently part of 16 AF/CC's responsibility to operate, secure, and defend the AFIN. AFI 10-701, para 6.7, describes how AIM products can be used. Breaches can be attributed to individual users and, unlike ESSA products, there is no restriction on the use of information gathered in an AIM mission in criminal or administrative adverse actions.

c) DOD Consent Banner. The consent banner is another element in CDA network monitoring and OPSEC missions. Users of all DOD information systems—including networks and telephones—expressly consent to the monitoring of their systems and communications within those systems for purposes of se-

curing the network and operational security. This express consent to monitoring precludes a reasonable expectation of privacy required for Fourth Amendment protections against warrantless searches and seizures. Federal courts have found that users who clicked on consent banners have no reasonable expectation of privacy.[11] See the current Air Force banner at https://federation.prod.cce.af.mil/.

3. Air Force Cyberspace Defense (ACD). ACD is designed to prevent, detect, respond to, and provide forensics of intrusions into unclassified and classified networks. The AFCERT uses ACD to deliver protection, detection, and response to users, including in-depth forensics and continuous monitoring and defense of Air Force networks. ACD uses intrusion detection and prevention systems at AFIN gateways. Operators can conduct active countermeasures against network intrusions and in-depth analysis to attribute threat actors and assess damage to the Air Force.[12] ACD operates in four subdisciplines:

   a) Incident prevention protection: conducting comprehensive vulnerability assessment, systematically identifying weaknesses, and assessing and proactively mitigating software and hardware vulnerabilities. The ACD weapon system protects AF III. Legal networks against new and existing malicious logic, and the ACD weapon system crew interfaces with the Air Force Office of Special Investigations during malicious logic-related incidents.

   b) Incident detection: monitoring classified/unclassified Air Force networks. ACD identifies and researches anomalous activity to determine threats to systems, monitors real-time alerts generated from network sensors, identifies and researches anomalous activities, and performs in-depth research of historical traffic reported through sensors.

   c) Incident response: conducting network incident response actions. ACD determines the extent of intrusions and develops courses of action to mitigate threats, verifies attribution, and restores affected systems and networks based on log and system analysis.

   d) Computer forensics: conducting in-depth analysis to characterize threats from identified incidents and suspicious activities,

followed by damage assessment. ACD supports the incident response process by capturing the full impact of exploits and reverse engineers code to determine the impact to the network and/or system.

4. Cyber Security and Control System (CSCS). CSCS provides 24/7/365 network mission assurance, network management, and defensive cyberspace operations for the AFIN as directed by USCYBERCOM and AFCYBER. CSCS operators conduct tactical-level cyberspace situational awareness and defend, manage, control access to, and monitor the Air Force Network (AFNET) and Air Force Secret Internet Protocol Router Network (SIPRNet) (Air Force Network – Secure) boundary. Additionally, CSCS operators respond to real-time events. Integrated Network Operations and Security Centers (I-NOSC), Enterprise Service Units (ESU), and Area Processing Centers (APC) are integral to the CSCS. I-NOSCs ensure the network is operational and fully capable; the ESUs operate, maintain, and monitor AFIN services; and APCs provide network application hosting and storage management to Airmen worldwide through Regional Data Centers. CSCS crews monitor, assess, and respond to real-time network events; identify and characterize anomalous activity; and take appropriate response actions when directed by the 616 OC.[13]

5. Cyberspace Vulnerability Assessment/Hunter (CVA/H). CVA/H enables execution of vulnerability, compliance, defense, and non-technical assessments, penetration testing (e.g., network intrusion analysis and systems vulnerability analysis), and Hunter missions on AF and DOD networks and systems. Hunter operations characterize and then eliminate advanced persistent threats (APT) to mission assurance. CVA/H focuses on the capability to find, fix, track, target, engage, and assess (F2T2EA) those APTs. During active engagements, the CVA/H weapon system provides a mobile precision protection capability to identify, pursue, and mitigate cyberspace threats. The CVA/H mission is to produce effects in, through, and from cyberspace by employing synchronized DCOs to prevent, detect, and respond to cyberspace intrusions. To achieve these effects, CVA/H is employed to conduct blue network vulnerability assessments, network intrusion analysis, and systems vulnerability analysis and defeat adversary activity.

6. The Cyber Command and Control Mission System weapon system (C3MS). C3MS provides C2 and situational awareness for Air Force–provided forces in support of CCMD missions and requirements. This system enables the AFCYBER and JFHQ-C commander to develop and disseminate cyber strategies and plans, then execute and assess these plans. C3MS provides 24/7/365 monitoring and control of Air Force core systems and mission system networks, cyber indications and warnings (I&W), and intelligence analysis for mission assurance. C3MS enables orders generation, processing, tracking, and execution (CTOs and MTOs) in conjunction with published air tasking orders (ATO) while assuring seamless integration of cyber effects with AOCs, MAJCOMs, and USCYBERCOM. The 616 OC uses C3MS to provide a common operational picture Air Force–wide. C3MS has five major subcomponents:

   a) Situational awareness: produces a common operational picture by fusing data from various sensors, data bases, weapon systems, and other sources to gain and maintain awareness of friendly, neutral, and threat activities that impact joint forces and the DAF.

   b) Intelligence, surveillance, and reconnaissance products: enable the integration of cyberspace I&W, analysis, and other actionable intelligence products into overall SA, planning, and execution.

   c) Planning: leverages situational awareness to develop long- and short-term plans, tailored strategy, and courses of action and shape execution of OCO, DCO, and DODIN ops.

   d) Execution: leverages plans to generate and track CTOs to employ assigned and attached forces in support of OCO, DCO, and DODIN ops.

   e) Integration with other C2 nodes: provides the ability to integrate Air Force–generated cyber effects with AFCYBER lines of effort, USCYBERCOM, and other C2 nodes.[14]

III. Legal Reviews of Weapons That Employ Cyber Capabilities and Reviews of Cyber Capabilities

A. A weapon requires a legal review consistent with DOD policy.[15] The DOD requires that "the acquisition and procurement of DOD weapons

and information systems must be consistent with all applicable domestic law, and the resulting systems must comply with applicable treaties and international agreements, . . . customary international law, and the law of armed conflict (also known as the laws and customs of war). An attorney authorized to conduct such legal reviews in the DOD must conduct the legal review of the intended acquisition of weapons or weapons systems."[16] The *Law of War Manual* provides that DOD policy requires the legal review of the acquisition of weapons or weapon systems. The assessment includes weapons that employ cyber capabilities to ensure they are not prohibited per se by the law of war. The manual clarifies that not all cyber capabilities constitute a weapon or weapons system. The DOD essentially defers to military departments to determine whether they want to implement regulations to address what cyber capabilities require legal review.[17] Currently, AFI 51-401, *The Law of War*, prescribes AF policy regarding cyber capabilities. It states that "an Air Force cyber capability . . . is any device, computer program or computer script, including any combination of software, firmware or hardware intended to deny, disrupt, degrade, destroy or manipulate adversarial target information, information systems or networks."[18] The AFI further delineates that AF cyber capabilities do not include capabilities internal to DOD use or training or solely intended to provide access to adversarial and targeted computers, information systems, or networks.[19] However, Air Force Policy Directive 51-4, *Operations and International Law*, and AFI 51-401 are under revision. Additionally, cyber capabilities "are developed based on environment assumptions and expectations about the operating conditions that will be found in the operating environment."[20]

B. Cyber capabilities are a separate category from weapons and nonlethal weapons. They are not explicitly designed or primarily employed to incapacitate or permanently injure personnel or material, nor are they designed to effect undesired damage to property, facilities, material, and the environment.[21] Rather, cyber capabilities are devices, computer programs, or scripts intended to yield a reliable effect of denial, disruption, degradation, destruction, or manipulation of adversarial target information, information systems, or networks during a conflict or military operations.

C. Presently, prior to the acquisition, development, or modification of any cyber capability, a legal review is required to ensure compliance

with domestic and international law, including the law of war.[22] Specifically, the Office of the Judge Advocate General (DAF/JA) must ensure that all non-special program cyber capabilities developed, bought, built, significantly modified, or otherwise acquired by the Department of the Air Force are reviewed for legality under domestic and international law prior to acquisition.[23] In rare cases where circumstances do not permit a legal review prior to acquisition or development, "a legal review must be accomplished prior to any employment in military operations."[24] The Office of the Secretary of the Air Force General Counsel (SAF/GCI), in coordination with the Department of the Air Force Operations and International Law Directorate (DAF/JAO), is responsible for ensuring the legality of all special program cyber capabilities.[25]

1. A legal review must consider any specific prohibitions in domestic or international law or prohibitions in accepted customary international law. It must also evaluate whether the cyber capability is calculated to cause unnecessary suffering or injury and can be directed against a specific military objective or, if not, is of a nature to cause damage or a significant adverse effect on military or civilian objectives without distinction.[26]

2. While not required, the legal review may note any legal issue that could affect an investment decision.[27] Finally, any legal review completed by another Service or the armed forces of another country may be considered in the DAF's determination of the legality of a cyber capability. However, the legal review conclusions of another Service or foreign armed forces are not binding for the purposes of the DAF's legal review. Rather, such opinions may be persuasive and incorporated by reference into the Department of the Air Force legal review. If such legal review is incorporated, DAF/JAO will provide and maintain a copy of the review.[28]

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Joint Publication (JP) 3-12, *Cyberspace Operations*, GL-5.
2. JP 3-12, GL-4.
3. JP 3-12, GL-4.
4. Department of the Air Force Instruction (DAFI) 17-130, *Cybersecurity Program Management*, para 3.4.3. Though some documents reference CSSP as cyber

security service provider and others as cybersecurity service provider, the terms are interchangeable.

5. JP 3-0, *Joint Operations*, GL-17.

6. For more information on why these are classified as weapon systems and additional descriptions of each, see Skinner, "Importance of Designating Cyberspace Weapon Systems," 29–48. As of publication, General Skinner is serving as the Defense Information Systems Agency (DISA) director.

7. AFINC training, evaluation, and procedures are outlined in Air Combat Command (ACC) manuals pending AFI rewrites. See ACC Manual (ACCMAN) 17-2AFINC, vol. 1, *Air Force Intranet Control (AFINC)—Cybercrew Training*; ACCMAN 17-2AFINC, vol. 2, *Air Force Intranet Control (AFINC)—Standardization/Evaluation Program*; and ACCMAN 17-2, vol. 3, *Air Force Intranet Control (AFINC) – Operations and Procedures*.

8. CDA training, evaluation, and procedures are outlined in ACCMAN 17-2CDA, vol. 1, *Cyberspace Defense Analysis (CDA)—Cybercrew Training*; ACCMAN 17-2CDA, vol. 2, *Cyberspace Defense Analysis (CDA)—Standardization and Evaluation (Stan/Eval)*; and ACCMAN 17-2CDA, vol. 3, *Cyberspace Defense Analysis (CDA)—Operations and Procedures*.

9. AFI 10-701, *Operations Security (OPSEC)*, chap. 6.

10. AFI 33-332, *Air Force Privacy and Civil Liberties Program*.

11. United States v. Larson, 66 M.J. 212 (C.A.A.F. 2008).

12. ACD training, evaluation, and procedures are outlined in ACCMAN 17-2ACD, vol. 1, *Air Force Cyberspace Defense (ACD)—Cybercrew Training*; ACCMAN 17-2ACD, vol. 2, *Air Force Cyberspace Defense (ACD)—Standardization/Evaluation Program*; and ACCMAN 17-2ACD, vol. 3, *Air Force Cyberspace Defense (ACD)—Operations and Procedures*.

13. CSCS training, evaluation, and procedures are outlined in AFI 17-2CSCS, vol. 1, *Cyberspace Security and Control System (CSCS)—Cybercrew Training*; AFI 17-2CSCS, vol. 2, *Cyberspace Security and Control System (CSCS)—Standardization/Evaluation Program*; and AFI 17-2CSCS, vol. 3, *Cyberspace Security and Control System (CSCS)—Operations and Procedures.*

14. Air Combat Command, "Cyber Command and Control Mission System (C3MS)."

15. DOD, *Law of War Manual*, sec. 6.2; and Department of Defense Directive (DODD) 5000.01, *Defense Acquisition System*.

16. DODD 5000.01, para. 1.2.v.

17. DOD, *Law of War Manual*, sec. 16.6.

18. AFI 51-401, *Law of War*.

19. AFI 51-401.

20. JP 3-12, *Cyberspace Operations*.

21. DODD 3000.03E, *DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*.

22. AFI 51-401, *Law of War*.

23. AFI 51-401, para. 5.

24. AFI 51-401, para. 5

25. AFI 51-401, para. 2.6

26. AFI 51-401, paras. 7.1–7.1.2.2.

27. AFI 51-401, para. 7.3. It is important to note that the AFI language is intended to liberally permit legal commentary on how employment of a developmental cyber capability may affect other investment and acquisition decisions for similar or related capability. See, for example, U.S. Government Accountability Office (GAO), *Weapon Systems Cybersecurity*.

28. AFI 51-401, *Law of War*, para. 7.2.

Chapter 6

Offensive Cyberspace Operations

I. Definition

Offensive cyberspace operations (OCO) are missions intended to project power in and through cyberspace.[1]

II. Legal Authorities

A. Constitutional Authorities. The President of the United States (POTUS), as commander in chief, has inherent authority to use military force to defend the U.S. under Article II of the U.S. Constitution.[2] The President may delegate these powers. The authority to act as an agent of the government must always derive from a chain of delegated authorities. POTUS's power is strongest when coupled with the express or implied will of Congress.[3]

B. U.S. Domestic Statutory Authorities. National Defense Authorization Act (NDAA). The NDAA for Fiscal Year (FY) 2012 provides that "the Department of Defense has the capability, and upon direction of the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests."[4] The NDAA for FY 2019 states that the DOD may "take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter . . . an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes."[5]

1. The NDAA for FY 2018 directed the SecDef to establish processes and procedures to integrate strategic information operations (military deception [MILDEC], public affairs, electronic warfare, and cyber ops) and to publish a DOD strategy for the same, including activities to counter and deter "malign actors."[6]

2. NDAA FY 2019, § 1631, made the following key changes to Title 10 (§ 394):

   a) The law directs the SecDef to prepare for and, when authorized, conduct cyber operations (including clandestine military activities) in defense of the U.S. and its allies in response to malicious cyber operations by a foreign power.[7]

b) The law authorizes military activities or operations in cyberspace "short of hostilities" and "in areas in which hostilities are not occurring including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States."[8]

c) The law also provides that "a clandestine military activity or operation in cyberspace shall be considered a traditional military activity."[9] A *cyberspace clandestine military* activity is defined as

> a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary that is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly; and is to be carried out as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or the Secretary; to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or in support of information-related capabilities.[10]

d) DOD doctrine defines *clandestine activities* as "operations sponsored or conducted by governmental departments in such a way as to assure secrecy or concealment" and includes "passive" intelligence collection and information gathering operations in cyberspace.[11]

1. Clandestine activities are distinguishable from "covert actions." Covert actions are "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[12] Covert actions are an intelligence activity and carry with them several congressional reporting requirements. Since clandestine military activities are military activities approved by the President, they are exempt from Title 50 reporting requirements.

2. The covert action statute describes how the intelligence community components receive Presidential authorization to conduct operations that are not attributable to the United States. "Traditional military activities" such as "clandestine activities" are exempt from this process. This inclusion of clandestine military cyber operations as a traditional military activity is a significant development because it denies the intelligence community the ability to object to and possibly thwart DOD's efforts to conduct non-attributable military cyber operations in gray-zone conflicts.

3. A key development in military cyber operations and national security activities writ large is the convergence of distinct operational concepts in the cyberspace domain. That is, military activity once occurring elsewhere is increasingly occurring in cyberspace. This trend is part of the larger movement toward Internet Protocol convergence, where Internet-based technology is the conduit for varying forms of human activity. Military information operations are an important flashpoint for this trend and explain the expanding definition of what constitutes military cyber operations.

4. Military information operations involve the use of "information-related capabilities" to achieve military ends.[13] These capabilities include "a variety of technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military information support operations (MISO), military deception (MILDEC), influence activities, operations security (OPSEC), and intelligence."[14] In other words, information operations span multiple disciplines and domains.

    a) One of the limiting principles of DOD information operations is its relationship to an authorized military purpose, either as a stand-alone effort or as an activity in support of other lines of effort occurring during a military operation. Another limiting principle is that military activity is generally publicly attributable to the government. Although there are exceptions to these principles, the military does not usually execute operations that seek to achieve other than a military purpose, and the United States publicly acknowledges its operations.

    b) Military cyberspace operations challenge these limiting principles. For obvious operational and technical reasons, military operations in cyberspace often cannot be publicly attributable

to the United States. Additionally, much military operational activity in cyberspace occurs in so-called gray-zone conflicts that do not always resemble military activities in areas of open hostilities. To account for these differences, military cyber operations have necessitated revised policy and legal frameworks that capture the evolving nature of military operations in the cyber domain.

3. 10 U.S.C. § 397 establishes the position of the principal information operations advisor, with the following responsibilities:

   a) Oversee policy, strategy, planning, resource management, operational considerations, personnel, and technology development across all elements of DOD information operations.

   b) Integrate and supervise the deterrence of, conduct of, and defense against information operations.

   c) Promulgate policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community, and other relevant federal government agencies and departments.

   d) Coordinate with the head of the Global Engagement Center to support the center's purpose, and liaison with the center and other relevant federal government entities to support such purpose.

   e) Establish and supervise a rigorous risk management process to mitigate the risk of potential exposure of United States persons to information intended exclusively for foreign audiences.

   f) Promulgate standards for the attribution or public acknowledgment, if any, of operations in the information environment.

   g) Develop guidance for and promote the capability of the DOD to liaison with the private sector and academia on matters relating to the influence activities of malign actors.

   h) Implement other such matters relating to information operations as the SecDef shall specify for purposes of this subsection.

III. Legal Analysis Common to All Cyber Operations

A. Domestic Law

1. Authority

a) Constitutional Article II in addition to congressional grants of authority; see 2001 Authorization for Use of Military Force and operations against Russia, China, North Korea, and Iran (FY19 NDAA §1642); NSPM-13.

b) Note: The Computer Fraud and Abuse Act (CFAA) does not constrain appropriately authorized DOD cyberspace operations under the analysis of *Nardone vs. the United States*.

2. Traditional Military Action (TMA) and Congressional Military Cyber Operations Oversight

a) Legislative history and 10 U.S.C. § 394 clarifications show cyber is TMA and not covert action.

b) Privacy and Civil Liberties

(1) Defense of elections cannot hinder First Amendment freedom of speech in relation to expression of political views.

(2) U.S. case law has three key strands: (1) The U.S. Government may incidentally burden the right to receive information from foreign sources without violating the First Amendment; (2) Courts have recognized a compelling government interest in protecting U.S. elections from certain types of foreign influence, especially when exercised covertly; and (3) Government action based on content of speech will be suspect.

(3) Based on these precedents, DOD lawyers analyzing cyberspace operations for First Amendment compliance consider factors including whether an operation is targeting foreign actors versus the information itself, the extent to which an operation may be "content neutral," and the foreign location and government affiliation of the target.

B. International Law

1. Use of Force

a) UN Charter art. 2(4) prohibits force on territorial integrity or political independence.

b) Exceptions include the inherent right of self-defense, and that includes cyber.

c) For cyber, the DOD considers whether an operation causes physical injury/damage that would be considered use of force if caused solely by traditional means like a missile or mine.

2. Principle of Non-Intervention

   a) This principle applies to elections and State views that disrupting the fundamental operation of a legislative body or destabilizing a financial system is a prohibited intervention.

   b) There is no international consensus on nonintervention, even outside of cyber. If a State consents to the intervention, there is no issue.

3. Countermeasures

   a) Countermeasures are generally available and traditionally require notice. Views vary about whether notice is required in all cyber cases because of secrecy or urgency. Notice may not be required in every case in a cyber context due to the practical concepts of secrecy or urgency applicable in cyberspace.[15]

   b) If it is not apparent that an act is internationally wrongful and attributable to a State in a time frame that the DOD must respond in, countermeasures would not be available.

4. Not a Use of Force or Prohibited Intervention

   a) According to the former DOD General Counsel, "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."[16]

   b) The above 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."

5. State Sovereignty

   DOD lawyers consider State sovereignty in cyber operations in that "States have sovereignty over the information and communications technology infrastructure within their territory." However, "the implications for sovereignty for cyberspace are complex." While the domain is continually evolving, there is no apparent rule that "all infringements on sovereignty in cyberspace necessarily involve violations of international law."[17]

6. Compliance with the Law of War in All Military Operations

   DOD policy is that "*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."[18]

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. Joint Publication (JP) 3-12, *Cyberspace Operations*, GL-5; and Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, s.v., "offensive cyberspace operations."
2. See Prize Cases, 67 U.S. (2 Black) 635 (1863).
3. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).
4. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).
5. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1642, 132 Stat. 1636, 2132 (2018).
6. See National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1637, 131 Stat. 1283, 1742 (2017).
7. See 10 U.S.C. § 394; *Accord* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(a).
8. 10 U.S.C. § 394(b); *Accord* War Powers Resolution, 50 U.S.C. § 1541.
9. 10 U.S.C. § 394(c).
10. 10 U.S.C. § 394(f)(A)-(B).
11. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, s.v. "clandestine operations."
12. 50 U.S.C. § 3093(a),(e).
13. Department of Defense Directive (DODD) 3600.01, *Information Operations*.
14. See DODD 3600.01.
15. Ney, "Remarks at U.S. Cyber Command Legal Conference."

16. Ney, “Remarks.”
17. Ney, “Remarks.”
18. Ney, “Remarks.”

Chapter 7

Cyber Intellectual Property

I. Technology Transfer

A. DOD Technology Transfer (T2) Program. DODI 5535.08 defines a *laboratory* and/or *technical activity* as a "facility or group of facilities owned, leased, or otherwise used by a Federal Agency, a substantial purpose of which is the performance of research, development, or engineering by employees of the Federal Government."[1]

B. Technology Executive Officer (TEO) Responsibilities. The TEO is assigned program management responsibilities for the Air Force Technology Transfer Program.[2] The officeholder is the reviewing authority for all cooperative research and development agreements (CRADA).[3] The TEO is also authorized to delegate reviewing authority to commanders and directors of laboratories and/or technical activities.[4]

II. Cooperative Research and Development Agreements

A. Statutory authorization was necessary to grant federal agencies the authority to accept funds from nonfederal entities and put those funds to use in support of the lab where they were received. Congress authorized CRADAs to facilitate the transfer of federally owned or originated technology to the private sector.[5]

B. Pursuant to the statutory authorization in 15 U.S.C. § 3710a, the DOD and the Air Force implemented instructions outlining the T2 process and the format of T2 agreements.[6] Like 15 U.S.C. § 3710a, DOD instructions provide that "DOD laboratories and/or technical activities may commit resources such as personnel, services, facilities, equipment, intellectual property or other resources with or without reimbursement, but shall not provide funds to the non-Federal partner as part of the agreement. Non-Federal parties may commit funds to the Federal partner to the agreement."[7]

C. CRADAs must conduct specified research and development efforts consistent with the missions of the laboratory or technical activity.[8] As a result, for any proposed CRADA, there must be a nexus to the laboratory's mission.

D. Other federal agencies can be brought into CRADAs as "other participants" as long as the laboratory signs a memorandum of agreement (MOA) with the other federal agency binding the latter to the terms of the CRADA.

E. All Air Force T2 activities must be accomplished utilizing a model agreement approved by the Office of the Deputy General Counsel (Acquisition) (SAF/GCQ).[9] The Air Force Model CRADA is mandatory. Substantive modification to any term or condition in the Model CRADA must be coordinated with and approved by SAF/GCQ.[10] Unlike Section I of the Model CRADA, the boilerplate that primarily serves to allocate intellectual property rights between the parties, Section II has more flexibility and is where the project itself is described. Section II cannot contradict Section I.

F. Packet Capture (PCAP) Data. The 67th and 688th Cyberspace Wings (CW) share Non-classified Internet Protocol Router PCAP data, captured by the 33rd Network Warfare Squadron's (33 NWS) sensors, with nonfederal parties through CRADAs with appropriate data privacy and security safeguards in place.

G. Data Breach Notification Requirements. Although not required by regulation, if an Air Force Activity is sharing Air Force data with a nonfederal entity through a CRADA, it is a best practice to require the nonfederal entity to report any event that compromises or has an actual or adverse effect on an information system containing Air Force data or the data residing therein. This requirement should be added to the Joint Work Plan (Section II) of the CRADA. At the end of December 2017, revisions to the Defense Federal Acquisition Regulation Supplement (DFARS) came into effect, requiring contractors and subcontractors to report cyber incidents to the DOD.[11] CRADAs are not subject to terms for procurement contracts and other instruments defined by 31 U.S.C. §§ 6303-305.[12] Therefore, the DFARS cyber incident reporting requirement does not apply to CRADAs.

H. The Air Force's Model. Air Force CRADA Version 5.2 (August 17, 2017) does not contain a data breach notification requirement. In 2019, 67 CW/JA (Judge Advocate) implemented data breach notification requirements across all 688 CW and 67 CW CRADAs. The 67 CW/JA has been working with the Air Force Research Laboratory and the DOD Cyber Crime Center (DC3) to add a mandatory data breach notification requirement to the next version of the Model CRADA.

I. Support to Critical Infrastructure. Through a CRADA, a laboratory can support critical infrastructure, such as a nearby energy company, by sharing PCAP data and providing training on cybersecurity tactics, techniques, and procedures (TTP). In turn, by hardening critical infrastructure defenses, the laboratory decreases the risk that operations downrange will be affected by hostile cyber operations being conducted against critical infrastructure. CRADAs must conform with the Posse Comitatus Act, codified in 18 U.S.C. § 1385, and not engage in law enforcement activities.

J. Risk Management Framework (RMF). Technologies brought into the Air Force via a CRADA are subject to the RMF. Under DODI 8510.01, an "authorization decision applies to a specifically identified [information system or platform information technology] and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DOD authorization decision is expressed as [an authorization to operate (ATO), an interim authorization to test (IATT), or a denial of authorization to operate (DATO)]. [An information or platform information technology] system is considered unauthorized if an authorization decision has not been made."[13] An "ATO with conditions" can only be issued with the permission of the responsible DOD component chief information officer.[14] An ATO with conditions "closely manages risk while allowing system operation. The ATOs with conditions should specify an [authorizing official] review period that is within 6 months of the authorization date."[15]

III. Digital Millennium Copyright Act of 1998 (DMCA)

A. The DMCA expanded copyright protections to include rules designed to prevent circumventing protections put in place by copyright holders. Under 17 U.S.C. § 1201(a)(1), "no person shall circumvent a technological measure that effectively controls access to a work protected under this title." Under 17 U.S.C § 1201(a)(2), "no person shall manufacture, import, . . . or otherwise traffic in any technology . . . that . . . (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under

this title; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title."

B. To "circumvent a technological measure" means to "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[16] A technological measure "effectively controls access to a work" when "the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[17]

C. However, there are exceptions to the DMCA's prohibitions. In 17 U.S.C. § 1201(e), there is an exception for "lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State." The exception defines *information security* as "activities carried out to identify and address the vulnerabilities of a government computer, computer system, or computer network."[18]

   1. There is a reverse engineering exception for purposes of achieving interoperability with other computer programs.[19]

   2. There is an encryption research exception, which requires, inter alia, the researcher to have "made a good faith effort to obtain authorization before the circumvention."[20]

   3. There is an exemption for certain acts of *security testing*, defined as "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network."[21] To qualify for the exemption, the information derived from the security testing needs to be solely used to promote the security of the owner or operator of such computer system or network, and the information derived from the security testing needs to be used or maintained in a manner that does not

facilitate copyright infringement or a violation of applicable law, including a violation of privacy or breach of security.[22]

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. DODI 5535.08, *DoD Technology Transfer (T2) Program*, E2.1.3.1; *Accord* 15 U.S.C. § 3710a(d)(2)(a).
2. AFI 61-301, *Domestic Technology Transfer Process*, para. 2.2.
3. AFI 61-301, para. 4.1.1.
4. AFI 61-301, para. 4.1.1.
5. See 15 U.S.C. §§ 3710, 3710a.
6. See DODI 5535.08, *DoD Technology Transfer (T2) Program*; see also AFI 61-301, *Domestic Technology Transfer Process*.
7. DODI 5535.08, para. 6.17.7.
8. See AFI 61-301, *Domestic Technology Transfer Process*, attach. 1.
9. AFI 61-301, para. 3.1.
10. AFI 61-301, para. 3.3.
11. 48 C.F.R. § 204.7300.
12. DODI 5535.08, *DoD Technology Transfer (T2) Program*, para. 6.17.2.
13. DODI 8510.01, *Risk Management Framework for DoD Information Technology*, encl. 6, para. 2(e)(4).
14. DODI 8510.01, encl. 6, para. 2(e)(4)(b).
15. DODI 8510.01, para. 2(e)(4)(b).
16. 17 U.S.C. § 1201(a)(3)(A).
17. 17 U.S.C. § 1201(a)(3)(A).
18. 17 U.S.C § 1201(e).
19. 17 U.S.C § 1201(f).
20. 17 U.S.C § 1201(g).
21. 17 U.S.C § 1201(j)(1).
22. 17 U.S.C § 1201(j)(3).

Chapter 8

Defense Support to Civil Authorities

I. Legal Authorities: Basic Framework

Presidential Policy Directive 8 (PPD-8), National Preparedness, aims to strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters.[1] PPD 8 created the national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the nation to achieve the goal. The system allows the nation to track the progress of our ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the nation's security. The National Preparedness System (NPS) is the integrated set of guidance, programs, and processes that enables the nation to meet the national preparedness goal. The Department of Homeland Security (DHS), through the Federal Emergency Management Agency (FEMA), created the NPS, which sets out national planning frameworks covering prevention, protection, mitigation, response, and recovery.

II. Defense Support of Civil Authorities (DSCA)

A. DSCA constitutes support provided by U.S. federal military forces, DOD civilians, DOD contract personnel, DOD Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in Title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

B. DOD supports the national planning response framework through DSCA, which is codified in 32 C.F.R. § 185 and implemented by DOD Publication 3-28, DOD Directive 3025.18, the 3025 series DOD manuals, and Chairman of the Joint Chiefs of Staff Defense Support of Civil Authorities Execute Orders (CJCS DSCA EXORD).[2]

C. DSCA is initiated by a request for DOD assistance from civil authorities or qualifying entities or when authorized by the President or Secretary of Defense. All requests for DSCA shall be written and shall include a commitment to reimburse the DOD under the Economy Act, the Stafford Act, or other reimbursement authority. Support may be provided on a nonreimbursable basis only if required by law or if both authorized by law and approved by the appropriate DOD official. All requests from civil authorities and qualifying entities for assistance are evaluated under the "CARRLL" factors:

1. C – Cost (including the source of funding and the effect on the DOD budget)
2. A – Appropriateness (whether providing the requested support is in the interest of the Department)
3. R – Risk (safety of DOD forces)
4. R – Readiness (impact on the DOD's ability to perform its other primary missions)
5. L – Legality (compliance with laws)
6. L– Lethality (potential use of lethal force by or against DOD forces)

III. Immediate Response Authority

A. The most common request for assistance (RFA) is immediate response authority (IRA). Federal and State immediate response should be a measure of last resort. Federal military commanders, heads of DOD Components, and/or responsible DOD civilian officials (collectively referred to as "DOD officials") have immediate response authority as described in DODD 3025.18. The directive states that in response to an RFA from a civil authority, under imminently serious conditions and if time does not permit approval from higher authority, DOD officials may respond immediately. They may temporarily employ resources under their control—subject to any supplemental direction from higher headquarters—to save lives, prevent human suffering, or mitigate serious property damage within the United States. Immediate response authority does not permit actions that would subject civilians to the use of military power that is regulatory, prescriptive, proscriptive, or compulsory.

B. An immediate response shall end when the necessity giving rise to the response is no longer present (e.g., when sufficient resources are available from State, local, and other federal agencies to respond adequately, and that agency or department has initiated response activities) or when the initiating DOD official or a higher authority directs an end to the response. The DOD official directing a response under immediate response authority shall reassess whether there remains a necessity for the DOD to respond under this authority as soon as practicable but, if immediate response activities have not yet ended, not later than 72 hours after the request for assistance was received."

C. Support provided under immediate response authority should be provided on a cost-reimbursable basis, where appropriate or legally required, but will not be delayed or denied based on the inability or unwillingness of the requester to make a commitment to reimburse the DOD.

D. The authority of State officials is recognized to direct a State immediate response using National Guard personnel under State command and control (including personnel in Title 32 status) in accordance with State law, but National Guard personnel will not be placed in or extended in Title 32 status to conduct State immediate response activities.

IV. The Stafford Act

A. The Robert T. Stafford Disaster Relief and Emergency Act, Pub. L. No. 100-707, 102 Stat. 4689 (1988) or Stafford Act grants statutory authority to provide an orderly and continuing means of assistance from the federal government to state and local governments in carrying out their responsibilities to alleviate the suffering and damage that result from such disasters.[3]

B. For purposes of the Stafford Act, an *emergency* is defined as "any occasion or instance for which, in the determination of the President, federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States."[4]

C. A *major disaster* is defined as "any natural catastrophe (including any hurricane, tornado, storm, high water, wind driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snow-

storm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President, causes damage of sufficient severity and magnitude to warrant major disaster assistance under the Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby."[5]

D. If a State anticipates that its resources may be exceeded, the Stafford Act allows the Governor to request assistance from the federal government. The Governor of an affected State may request the declaration of a major disaster or emergency and must demonstrate, as a prerequisite for receiving assistance, both that the State's response plans have been activated and State and local capabilities are inadequate for effective response. The federal government becomes involved with a response when federal interests are involved; when state, local, tribal, or territorial resources are overwhelmed, and federal assistance is requested; or as authorized or required by statute, regulation, or policy.

V. The Economy Act

A. The Economy Act, 31 U.S.C. § 1535, allows federal agencies to provide support to other federal agencies on a reimbursable basis, unless the support is provided in the normal course of training or operations or the support results in a substantially equivalent training value.

B. The Economy Act authorizes interagency orders between federal agencies. The ordering agency must reimburse the performing agency for the costs of supplying goods or services. 31 U.S.C. § 1536 specifically indicates that the servicing agency should credit monies received from the ordering agency to the "appropriation or fund against which charges were made to fill the order."[6]

VI. Legal Authorities: Basic Framework + Cyber

A. Presidential Policy Directive-41 sets forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities.[7] PPD-41 complements and builds upon PPD-8 by integrating cyber and traditional preparedness efforts to manage incidents that include cyber and physical effects.

B. A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

C. A significant cyber incident is a cyber incident (or group of related cyber incidents) 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.

D. PPD-41 articulates various federal government agencies' roles and responsibilities during a cyber incident and a significant cyber incident. When a cyber incident affects a private entity, the federal government typically will not play a role in this line of effort.

   1. The Department of Justice, acting through the Federal Bureau of Investigation and National Cyber Investigative Joint Task Force, is the lead federal agency for threat response during a significant cyber incident. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site, collecting evidence and gathering intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing courses of action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

   2. The Department of Homeland Security, through the National Cybersecurity and Communications Integration Center (NCCIC), is the lead federal agency for asset response during a significant cyber incident. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing

and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

3. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the lead federal agency for intelligence support and related activities during a significant cyber incident. Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

VII. Defense Support to Cyber Incident Response (DSCIR) or Cyber DSCA

A. Building upon PPD-8 and DODD 3025.18, DOD also implements PPD-41.[8] This interim policy provides supplementary policy guidance, assigns responsibilities, and details procedures for providing DSCIR. It is currently set to expire in June 2021 while being converted to a new DOD issuance.

B. DSCIR may be provided using DOD military, civilian, and contractor personnel. The use of National Guard personnel for DSCIR in Title 32 is consistent with DOD policy.

C. Requests for DSCIR will be evaluated consistent with the criteria established in DODD 3025.18, with emphasized consideration given, but not limited to, the impact on DOD networks, systems, and capabilities if the support were to be provided. DSCIR may include direct on-location support, remote support, or a combination of both as appropriate. Requests for assistance for DSCIR will be considered only if they include both of the following:

   1. 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.

   2. Written permission for the DOD to access appropriate information and information systems (e.g., applicable hardware, software, networks, servers, Internet Protocol addresses, and databases).

VIII. Immediate Response Authority and DSCIR.

DSCIR to save lives, prevent human suffering, or mitigate serious property damage may be provided under immediate response authority in accordance with DODD 3025.18, but only in response to a request for assistance from a lead federal department or agency for asset response or threat response outside the DOD Information Network (DODIN) (as described in PPD-41).

IX. State Active Duty

A. State Active Duty (SAD) personnel are strictly militia status, funded and controlled entirely by the State. The States control all limits and authorities for their utilization. Generally, DOD and Service guidance do not apply unless there is the use of federal money, such as for equipment. When National Guard units or personnel are not under federal control, they report to the Governor of their respective State or territory or to the District of Columbia. Each of the 54 National Guard organizations is supervised by the Adjutant General (TAG) of the State or territory, who normally exercises command of its National Guard personnel for the State Governor. Under State law, the National Guard provides for the protection of life and property and the preservation of peace, order, and public safety. Personnel in SAD are State employees and should be treated as such. The Governor often uses SAD as first response to an incident.

B. Cyberspace equipment or programs may be limited to federal use for federal systems and therefore would not be authorized for State use in a SAD or outside of the DODIN. Executive Orders 12968 and 13549 as amended and DOD implementing guidance govern access and use of DOD information networks, software, hardware, systems, tools, tactics, techniques, and procedures beyond the classification level of Secret and is prohibited in SAD.[9]

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. See Presidential Policy Directive 8 (PPD-8), *National Preparedness*.

2. Joint Publication (JP) 3-28, *Defense Support of Civil Authorities*; see also DOD Directive (DODD) 3025.18, *Defense Support of Civil Authorities*.

3. 42 U.S.C. §§ 5121 *et seq*.

4. 42 U.S.C. § 5122(1).

5. 42 U.S.C. § 5122(2).

6. This process is further explained in DOD 7000.14-R, *Financial Management Regulation*, vol. 11A, *Reimbursable Operations Policy*, chap. 3.

7. See PPD-41, *United States Cyber Incident Coordination*.

8. See Directive-Type Memorandum (DTM) 17-007, "Interim Policy and Guidance for Defense Support to Cyber Incident Response."

9. See Executive Order (EO) No. 12968, 60 Fed. Reg. 40,425; see also EO No. 13549, 75 Fed. Reg. 51,609.

Chapter 9

Cyberspace Criminal Law

I. Constitutional Considerations

A. First Amendment. As Internet platforms increasingly become the public square of modern political discourse, traditional ways of understanding and regulating speech have been challenged. Private companies now have an outsized role in determining the value of certain kinds of speech, absorbing a role that in the past has been the domain of courts and publicly accountable government officials. The role of government in this process is uncertain.[1] In recent Court rulings, under the First Amendment, a public official's social media platform could be deemed a public forum if the account is accessible to the public at large and is used by a public official in an official capacity for official purposes.[2] While social media is an evolving area of law, early signs indicate that official social media accounts (such as a wing commander's Facebook page) may be deemed a public forum if they are open to the general public and if anyone can comment on a site where comments are permissible.[3]

B. Fourth Amendment

1. The third-party doctrine, as originally identified, holds that when individuals voluntarily turn information over to a third party, they have a reduced expectation of privacy for that information.[4] Thus, the Supreme Court has held that information such as the numbers dialed on a telephone (non-content information) or bank records lacks a reasonable expectation of privacy. However, the third-party doctrine has been turned upside down in light of recent Supreme Court precedent broadening the application of the Fourth Amendment to data that Americans voluntarily give to Internet service providers, cell phone companies, and other private businesses handling customer data.[5] Further, military courts are now a recognized jurisdiction for purposes of the Stored Communications Act (SCA), the primary mechanism for federal government access to privately held electronic data.[6] The kind of legal process required under this statute depends on the nature of the data (i.e., content versus non-content), but there are several caveats to this general principle.

2. Government-owned networks and systems are treated differently. The Air Force does not recognize an expectation of privacy on the Air Force Information Network (AFIN), communicated to users in the Notice and Consent Banner they must acknowledge whenever accessing an AFIN system. These consent and notification banners almost always satisfy Fourth Amendment or any similar statutory privacy protections for government-owned networks. This does not mean local network administrators can do whatever they want on Air Force systems. When in doubt, consult Sixteenth Air Force and other subject matter experts before advising commanders on the scope of their authority on local networks. For further information, contact 67 CW/JA for course materials for the Undergraduate Cyber Course (often referred to as Cyber 100) and related current guidance.

C. Fifth Amendment. The privilege against self-incrimination in the military context has evolved to capture post-invocation questioning related to cell phone passwords and other forms of digital encryption.[7] The analyses in these cases are heavily fact-specific, and it is recommended that law professionals contact military justice experts for assistance with case law in this area.

II. Statutory Considerations

A. Electronic Communications Privacy Act

1. Wiretap Act (18 U.S.C. § 2511). The act prohibits the intercept of electronic communications without a warrant. Exceptions are collections under the Foreign Intelligence Surveillance Act (FISA), service-related monitoring by a service provider, or user consent. The Wiretap Act prohibits the intentional interception of, attempt to intercept, or procurement of another to intercept any wire, oral, or electronic communication.[8]

   a) Electronic Communications. Electronic communications are defined expansively.[9] Wiretap Act prohibitions extend to the use of any device to intercept any oral communication, the disclosure or use of any communication known to have been intercepted in violation of the act, or the disclosure of any communication obtained in a criminal investigation where there is intent to interfere with the investigation.[10] The act only prohibits recording the oral communications of a person who has a

reasonable expectation that the communication will not be subject to interception.[11] For example, if loud conversation occurs in a small room in the presence of others that the speaker has no right to exclude, there is no reasonable expectation of privacy.[12] However, the act does not regulate silent video surveillance, as the surveilled activity does not constitute a communication.[13] Finally, applicability of the Wiretap Act is determined by where the interception occurred, not the route the communication took.[14] Even if an intercepted communication travels through parts of a U.S.-based communication system, the Wiretap Act does not apply outside the United States if the interception occurs outside the country.[15]

b) Applicability. The Wiretap Act does not apply to communications in electronic storage, as this does not constitute an interception.[16] However, the Wiretap Act does apply to interception of an email in temporary electronic storage that is intrinsic to the communication process.[17] Similarly, a website must be intercepted during transmission and not while in electronic storage.[18] The Wiretap Act does not apply to Internet Protocol addresses and uniform resource locators, as they identify the devices and do not constitute the contents of the communication.[19] The act does not affect the acquisition of foreign intelligence from international or foreign communications by the United States Government otherwise conducted in accordance with applicable federal law.[20]

c) Exceptions. An employee of a service provider whose facilities are used to transmit wire or electronic communications may intercept, disclose, or use a communication in the normal course of business necessary to render service or to protect the service provider.[21] Since the Air Force is not a provider of wire communications to the public, it may observe the service or randomly monitor communications.[22] Similarly, a person may intercept wire or electronic communications if the communication is causing harmful interference to any lawfully operating station or consumer electronic equipment, but only to the extent necessary to identify the source of the interference. Notably, the exceptions available to a service provider are narrower under the Wiretap Act than under the Stored Communication

Act.[23] Under the Wiretap Act, there must be a nexus between the monitored activity and these service provider exceptions.

(1) A person acting under the color of law may intercept a communication where the person is a party to the communication or the party to the communication has given prior consent.[24] A person acting under the color of law may intercept a wire or electronic communication of a computer trespasser transmitted to, though, or from a computer if the owner consents, the person is lawfully engaged in an investigation, the person has reasonable grounds to believe the communications will be relevant to the investigation, and only the communications to or from the trespasser are acquired.[25] A person not acting under the color of law may intercept a communication where the person is a party to the communication or the party to the communication has given prior consent, provided the interception is not for the purpose of committing a criminal or tortious act.[26]

(2) A person may intercept electronic communications if the communication is configured such that it is readily accessible to the general public.[27] A person may also intercept a radio communication for use by the general public or that relates to a person or vehicle in distress.[28] However, Wi-Fi communications are not readily accessible to the general public.[29]

2. Stored Communications Act (18 U.S.C. § 2701)

a) As noted above, the Electronic Communications Privacy Act (ECPA or Wiretap Act), Pub. L. No. 99-508, 100 Stat. 1848, is designed to protect private "in transit" information. The statute's purpose is to protect information that the communicator took steps to keep private.[30] Cases interpreting the federal SCA underscore that information is protectable as long as the communicator actively restricts the public from accessing the information.[31] The Wiretap Act grants protections above the Fourth Amendment, but there are several exceptions, including consent and communications readily accessible to the general public.[32]

b) The Stored Communications Act, Title II of the ECPA, was created to address "access to stored wire and electronic communications

and transactional records."[33] The SCA prohibits unauthorized access of stored wire and electronic communications and records intended to be private.[34]

(1) In interpreting what constitutes an intent to be private, the Department of Justice's position is that the SCA is intended to address computer hackers and corporate spies and not to criminalize access to "electronic bulletin boards" or information otherwise available to the general public. In short, if a "person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy[,] . . . access[ing] a communication on such a system is not a violation of the law."[35]

(2) A recent New Jersey case, *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659 (2013), found that SCA protections applied to nonpublic Facebook posts. The case addressed an employee terminated based, in part, on her Facebook posts, which a Facebook friend provided to her employer. The Court found that the Facebook posts fell under the SCA because her account was configured to be private, and the Facebook server stored the communication once it was posted.[36] However, the Court also concluded that the Facebook friend was an "authorized user," and, consequently, the friend's provision of the posts to her employer was not a violation of the law because the employer had not directed him to provide the information.[37] In short, if the public can readily access the information, such access by individuals is not criminal.

(3) Courts have held that even in the case where there is "an express warning, on an otherwise publicly accessible webpage," such warnings are, nevertheless, insufficient to give rise to SCA protections.[38] Thus, determining whether an SCA violation occurred depends almost exclusively on the user's privacy settings.[39]

3. Pen Register/Trap and Trace (18 U.S.C. § 3121). This statute prohibits warrantless capture of outgoing/incoming dialing, routing, addressing, or signaling information. Exceptions are the FISA, provider operation and maintenance, and consent. 18 U.S.C. § 3121 also broadly prohibits the warrantless installation or use of

a device to capture outgoing or incoming dialing, routing, addressing, or signaling information. This prohibition includes capturing the information from email communications.[40]

a) A pen register is a device or process that records or decodes outgoing information provided the recorded or decoded information does not include the content of the communication. It does not include a device used by a service provider or customer for billing purposes or other like purposes in the ordinary course of business.[41] A trap and trace device is a similar device or process that captures incoming information identifying the originating number or other information identifying the source of the communication provided the content of the communication is not included.[42] However, caller ID is not a trap and trace device.[43]

b) An electronic or wire communication service provider may use a pen register or trap and trace device when its use relates to protecting the rights or property of the provider, the operation of the service, or the service users from abuse of the service or for recording the initiation and completion of communications to protect against the abusive use of the service or where the service user consents.[44]

c) The law includes several limitations. A government agency may install or use a pen register or trap and trace device provided it uses technology reasonably available to it to restrict the information collected to dialing, routing, addressing, and signaling information and not to collect the content of the communication.[45] For example, the government may not seek cell site information pursuant to 18 U.S.C. § 3121 because the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010, forbids service providers from disclosing the physical location of a subscriber when the government proceeds with only the authority for pen registers and trap and trace devices.[46]

B. Computer Fraud and Abuse Act

1. Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030). It is a violation of criminal law to access a computer without authorization or when exceeding one's authorization. As noted above, much of the boundary and domain is contracted. Look at the contract, as

the DOD does not own all the DODIN but may be authorized to exercise several rights on the same. Since the DOD is moving away from data centers to storing information in cloud servers, putting our cyber teams on non-DOD owned networks implicates this statute. There are several court cases that help frame the boundaries and application of the CFAA.

a) *Nardone v. United States*, 302 U.S. 379 (1937). In *Nardone*, the Supreme Court concluded that U.S. Government agents were covered by a statute that allowed "no person" to engage in wiretapping.[47] The Court acknowledged the canon of statutory construction that the "general words of a statute do not include the government or affect its rights unless the construction be clear and indisputable upon the text."[48] The Court limited the application of the rule to two classes of cases. The first is "where an act, if not so limited, would deprive the sovereign of a recognized or established prerogative title or interest."[49] The second is where reading a statute to include governmental officers "would work obvious absurdity as, for example, the application of a speed law to a policeman pursuing a criminal or the driver of a fire engine responding to an alarm."[50] This reasoning, for example, is why the U.S. Government may engage in offensive cyber operations against adversary States.

b) *United States v. Cotterman*, 709 F.3d 952 (9th Cir., 2013). In *Cotterman*, the Ninth Circuit Court of Appeals held that a forensic examination of a traveler's digital device by U.S. Customs and Border Patrol agents required reasonable suspicion. While the Court acknowledged that border searches are a "narrow exception" to the Fourth Amendment, it considered a forensic examination of a digital device to be so intrusive that it must require some particularized suspicion on behalf of the agents conducting the search. In its analysis, the Court stated that a cursory review of a digital device, such as requesting that a traveler simply power on the device and show the agent what it contains, may be permissible without reasonable suspicion. However, the Court recognized that digital devices have evolved over the years to contain the most intimate details of a person's life and that conducting an in-depth forensic review of devices goes beyond the Fourth Amendment's reasonableness requirement and therefore requires reasonable suspicion.

c) *Riley v. California*, 395 U.S. 752 (2014). In *Riley*, the Supreme Court unanimously held that searches of digital information on a cell phone do not fit within the "search incident to arrest" exception to the Fourth Amendment and therefore require a separate warrant. While the Court acknowledged that a phone's physical aspects could be searched to ensure that it could not be used as a weapon, the digital information stored on the phone could not. Similar to *Cotterman*, the Court discussed how digital device technology has significantly advanced and why the immense storage capacity of cell phones results in a person's reasonable expectation of privacy protected by the Fourth Amendment.

d) *Mondelez International, Inc. v. Zurich American Insurance Co.*, 2018 WL 4941760 (Ill.Cir.Ct., 2018). *Mondelez* is a pending Illinois Circuit Court trial stemming from an insurance dispute. While the case is still pending trial and has yet to result in a precedent, it is a preview of the potential impact of the increase of digital conflict on the insurance industry and private companies. According to the complaint, in 2017 the plaintiff, Mondelez, Inc. was a victim of the NotPetya malware, which rendered many of its servers permanently dysfunctional and subsequently resulted in financial losses exceeding $100 million. Mondelez, Inc. filed an insurance claim with Zurich for the damages citing the policy clause that covered "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction." Zurich eventually denied the claim, citing the part of the policy document that bars payment of claims for damages resulting from "a hostile or warlike action . . . by any government or sovereign power . . . or agent or authority [thereof]." Zurich presumably based this denial on the U.S. Government's attribution of the NotPetya malware to the Russian government. Mondelez filed suit for breach of the insurance contract. The eventual outcome of the case will likely impact the future of the cyberattack insurance market.

e) *Van Buren v. United States*, 141 S. Ct. 1648 (2021). *Van Buren* narrowed the potential scope of the CFAA significantly by partially answering the question of what constitutes unauthorized access.[51] Prior to this case, there was a question as to whether the violation of a policy or term of service could constitute

unauthorized access. In *Van Buren*, the court used a "gates" analysis to help answer this question. In this context, a gate is a technical barrier that prevents access (or further access) to a network or portion of that network. This is opposed to mere policy or term of service that states no further access is authorized. If a person manages to bypass a "closed" gate through some form of hacking, then they have violated the CFAA. However, if the gate is "open" from a technical standpoint and a person accesses that system, they cannot be guilty of a CFAA violation. Thus, a mere violation of a company policy or term of service cannot, on its own, constitute a CFAA violation.

f) Under 18 U.S.C. § 1030(f), there is a key carve-out: "This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."

2. Article 123 of the Uniform Code of Military Justice (UCMJ) and the Computer Fraud and Abuse Act. Military activities in cyberspace implicate potential UCMJ violations. Article 123 prohibits the unauthorized access of government computers under a variety of circumstances, similar to the prohibitions found in the CFAA. Although the statutes use comparable language, the scope of their prohibitions differ.

   a) The CFAA, as amended, was meant to protect U.S. Government computers and critical banking thieves and hackers and does not limit the President directing military actions in cyberspace when conducting properly authorized military cyber operations abroad against foreign actors.[52] However, military practitioners should proceed with caution in indicating that the CFAA does not apply to a cyber operation because it likely requires the action to be both abroad and against known foreign actors.

   b) There is no "hacking back" exception mentioned in the CFAA or Article 123. Although there are no examples of prosecution of a victim of a computer crime for attempting to unilaterally respond to a malicious cyber operation by accessing the offender's computers or third-party computers, the Department of Justice (DOJ) has published guidance discouraging hacking back.[53] The DOJ warns that if a victim organization accesses, modifies,

or damages a computer it does not own or operate, even if the computer appears to have been involved in an attack or intrusion, the victim organization, regardless of motive, may violate the CFAA.[54]

c) In practice, organizations can use a spectrum of defensive measures, carrying different levels of CFAA risk with respect to prosecutorial discretion. Passive defenses that operate entirely within one's own network, such as firewalls and honeypots, are considered legal. Depending on how they operate, beacons placed inside an individual's data are considered technical violations of the CFAA that would be unlikely to be prosecuted (to "beacon" home, the code would need to access the adversary's computers). Actions that could foreseeably cause destruction, denial, or degradation to the adversary's or third-party computers are considered to incur a higher risk of triggering the DOJ's prosecutorial discretion, such as "poisoning" the data with malicious code to harm the adversary's computer or attempting to locate and destroy the stolen data on the adversary's computer.

3. Clarifying Lawful Overseas Use of Data (CLOUD) Act. The United States enacted the CLOUD Act in March 2018 to speed access to electronic information held by U.S.-based global providers that is critical to our foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime.[55] The CLOUD Act authorizes bilateral agreements between the United States and trusted foreign partners that will make both nations' citizens safer, while at the same time ensuring a high level of protection of those citizens' rights.[56]

4. Other statutes that have applicability in cyber law include wire fraud, 18 U.S.C. § 1343; identity fraud, 18 U.S.C. § 1028; identity theft, 18 U.S.C. § 1028A; access device fraud, 18 U.S.C. § 1029; theft of government property, 18 U.S.C. § 641; unauthorized interception of communications, 18 U.S.C. § 2511; and provisions relating to espionage and protection of defense information, 18 U.S.C. §§ 793-798.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the references section.)

1. See U.S. Const. amend. I.
2. Knight First Amendment Institute v. Trump, 928 F.3d 226, 568-570 (2d. Cir. 2019) (President's Twitter account is a public forum because it is open to the public at large and used by the President in an official capacity, so viewpoint discrimination by blocking users is not permitted).
3. Knight First Amendment Institute v. Trump, 928 F.3d 226, 568-570 (2d. Cir. 2019). See also Davison v. Randall, 912 F.3d 666, 681 (4th Cir. 2019) (Chairman of County Board of Supervisors cannot delete a critical constituent's comments on a public Facebook page used in an official capacity).
4. See Smith v. Maryland, 442 U.S. 735 (1979).
5. See Carpenter v. United States, 138 S. Ct. 2206 (2018).
6. See 18 U.S.C. § 2711(3)(c).
7. See U.S. Const. amend. IV. See also United States v. Robinson, 77 M.J. 303 (C.A.A.F. 2018); and United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017).
8. 18 U.S.C. § 2511(1)(a).
9. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
10. 18 U.S.C. §§ 2511(1)(b), (c), (d), (e).
11. United States v. Dunbar, 553 F.3d 48 (1st Cir. 2009).
12. Kemp v. Block, 607 F. Supp. 1262 (D. Nev. 1985).
13. United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992).
14. United States v. Cotroni, 527 F.2d 708 (2d Cir. 1975).
15. United States v. Cotroni, 527 F.2d 708 (2d Cir. 1975).
16. Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).
17. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
18. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).
19. *In re* Nickelodeon Consumer Privacy Litig., No. 2443 (SRC), 2014 U.S. Dist. LEXIS 91286 (D.N.J. July 2, 2014).
20. 18 U.S.C. § 2511(2)(f).
21. 18 U.S.C. § 2511, (2)(a)(i).
22. 18 U.S.C. § 2511, (2)(a)(i).
23. Stevens and Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*; and 18 U.S.C. §§ 2701–2712.
24. 18 U.S.C. § 2511(2)(c).
25. 18 U.S.C. § 2511, (2)(i).
26. 18 U.S.C. § 2511, (2)(d).
27. 18 U.S.C. § 2511, (2)(g)(i).
28. 18 U.S.C. § 2511, (2)(g)(ii).
29. Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013).
30. 18 U.S.C.S. § 2511(2)(g)(i).

31. 18 U.S.C.S. §§ 2701-2711.

32. 8 U.S.C. § 2511(2)(c)-(d); 18 U.S.C. § 2511(2)(g)(i).

33. See Pub. L. No. 99-508, 541, at 3 (1986).

34. 18 U.S.C. § 2701(a); and 18 U.S.C. § 2707.

35. 18 U.S.C. § 2701(a). See also Department of Justice (DOJ), *Criminal Resource Manual,* § 1061.

36. DOJ, § 668.

37. DOJ, §§ 670-671.

38. See, for example, Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006).

39. See, for example, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

40. *In re* U.S. for Orders Authorizing Installation & Use of Pen Registers, 416 F. Supp. 2d 13 (D.D.C. 2006).

41. 18 U.S.C. § 3127(3).

42. 18 U.S.C. § 3127(4).

43. Sparshott v. Feld Entertainment, Inc., 354 U.S. App. D.C. 63, 311 F.3d 425 (2002).

44. 18 U.S.C. § 3121(b),

45. 18 U.S.C. § 3121(c).

46. *In re* United States of Am. for an Order Authorizing the Installation & Use of a Pen Register, 402 F. Supp. 2d 597 (D. Md. 2005).

47. Nardone v. United States, 302 U.S. at 383-84.

48. 302 U.S. at 383.

49. 302 U.S. at 383.

50. 302 U.S. at 384.

51. Van Buren v. United States, 141 S. Ct. 1648 (2021).

52. Ney, "DOD General Counsel Remarks at the U.S. Cyber Command Legal Conference."

53. See DOJ, *Best Practices for Victim Response and Reporting of Cyber Incidents*, Ver. 2.0.

54. DOJ, *Best Practices*.

55. See Stored Communications Act, 18 U.S.C. § 2703 (2020); and Clarifying Lawful Overseas Use of Data Act, H.R. Res. 1625, 115th Cong. (2018), div. V, §§ 103–106 [hereinafter CLOUD Act].

56. For the full text of the CLOUD Act, see DOJ, Cloud Act Resources website; and DOJ, *Promoting Public Safety, Privacy, and the Rule of Law*.

Abbreviations

ACC	Air Combat Command
ACC/CC	Commander, Air Combat Command
ACD	Air Force Cyberspace Defense
AF	Air Force
AFCERT	Air Force Computer Emergency Response Team
AFCYBER	Air Forces Cyber/Sixteenth Air Force
AFI	Air Force instruction
AFIN	Air Force Information Network
AFINC	Air Force Intranet Control
AFNET	Air Force Network
AFNET-S	Air Force Network – Secure
AFOSI	Air Force Office of Special Investigations
AFPD	Air Force policy directive
AFRICOM	United States Africa Command
AI	artificial intelligence
AIM	active indicator monitoring
AO	authorizing official
AOC	air operations center
AOR	area of responsibility
AP	Additional Protocol
APC	Area Processing Center
APL	Approved Products List
APT	advanced persistent threat
ARCYBER	Army Cyber Command/2nd Army
ATC	Approval to Connect
ATO	authorization to operate
AWS	Amazon Web Services
BIPS	boundary intrusion prevention system

CAC	Common Access Card
CC	commander
CCDR	combatant commander/unified combatant commander
CCMD	combatant command/unified combatant command
CDA	cyber defense analysis
CDRAFCYBER	Commander, Air Forces Cyber
CDRUSCYBERCOM	Commander, United States Cyber Command
CENTCOM	United States Central Command
C.F.R.	*Code of Federal Regulations*
CI	counterintelligence
CI/KR	critical infrastructure and key resources
CIL	customary international law
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCS DSCA EXORD	CJCS Defense Support of Civil Authorities Execute Order
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CMF	Cyber Mission Force
CMT	combat mission team
CNMF	Cyber National Mission Force
CNSS	Committee on National Security Systems
CO	cyberspace operations
COASTGUARD CYBER	Coast Guard Cyber Command
COCOM	combatant command authority
CO-IPE	Cyberspace Operations – Integrated Planning Element
CONUS	continental United States
CPF	Cyber Protection Force
CPT	cyber protection team
CRADA	cooperative research and development agreement
CSCS	Cyber Security and Control System

CS-I	Cyber Squadron Initiative
CSP	Cloud Service Provider
CSSP	cybersecurity service provider
CST	cyber support team
C3MS	Cyber Command and Control Mission System
CTO	cyber tasking order
C2	command and control
CUI	controlled unclassified information
CVA/H	Cyberspace Vulnerability Assessment/Hunter
CW	cyberspace wing
DACO	directive authority for cyberspace operations
DAF	Department of the Air Force
DAF/JA	Department of the Air Force Office of the Judge Advocate General
DAF/JAO	Department of the Air Force Operations and International Law Directorate
DAFPD	Department of the Air Force policy directive
DATO	denial of authorization to operate
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations–internal defensive measures
DCO-RA	defensive cyberspace operations–response actions
DC3	Defense Cyber Crime Center
DEPORD	deployment order
DFARS	Defense Federal Acquisition Regulation Supplement
D4M	deny, degrade, disrupt, destroy, or manipulate
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIRNSA	director, National Security Agency
DISA	Defense Information Systems Agency

DISN	Defense Information Systems Network
DMCA	Digital Millennium Copyright Act of 1998
DNS	Domain Name System
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIN	Department of Defense Information Network
DODIN Ops	Department of Defense Information Network Operations
DOJ	Department of Justice
DSCA	Defense Support of Civil Authorities
DSCIR	Defense Support to Cyber Incident Response
DTM	directive-type memorandum
ECPA	Electronic Communications Privacy Act
eMASS	Enterprise Mission Assurance Support Service
ESSA	electronic system security assessment
ESU	Enterprise Service Unit
EUCOM	United States European Command
EXORD	execute order
FEMA	Federal Emergency Management Agency
FFP	firm-fixed-price (contract)
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Modernization Act
FLTCYBER	Fleet Cyber Command/10th Fleet
F2T2EA	find, fix, track, target, engage, and assess
FY	Fiscal Year
GFMIG	Global Force Management Implementation Guidance

HAF	Headquarters Air Force
HIPS	host intrusion prevention systems
HUMINT	human intelligence
IAB	Internet Architecture Board
IAC	international armed conflict
I&W	indications and warnings
IATT	interim authorization to test
IC	intelligence community
ICANN	Internet Corporation for Assigned Names and Numbers
ICJ	International Court of Justice
ID/IQ	indefinite delivery/indefinite quantity
IGE	international group of experts
I-NOSC	Integrated Network Operations and Security Center
IoT	Internet of Things
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IRA	immediate response authority
ISP	Internet service provider
IT	information technology
JA	judge advocate
JAIC	Joint Artificial Intelligence Center
JEDI	Joint Enterprise Defense Infrastructure
JFHQ-C	Joint Force Headquarters – Cyberspace
JFHQ-DODIN	Joint Force Headquarters – Department of Defense Information Network
JP	joint publication
JRSS	Joint Regional Security Stack
JWCC	Joint Warfighter Cloud Capability
JWICS	Joint Worldwide Intelligence Communications System

LoW	law of war
LOWM	*Law of War Manual*
MAJCOM	major command
MARFORCYBER	Marine Forces Cyber Command
MCCC	MAJCOM Communications Coordination Center
MCEN	Marine Corps Enterprise Network
MDT	mission defense team
MILDEC	military deception
MISO	military information support operations
MOA	memorandum of agreement
MTFP	mission-tailored force package
MTO	maintenance tasking order
NCCIC	National Cybersecurity and Communications Integration Center
NDAA	National Defense Authorization Act
NEN	Naval Enterprise Network
NGEN	Next Generation Enterprise Network
NIAC	non-international armed conflict
NIPRNet	Nonsecure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMCI	Navy/Marine Corps Intranet
NMT	national mission team
NORAD	North American Aerospace Defense Command
NORTHCOM	United States Northern Command
NPS	National Preparedness System
NSA	National Security Agency
NSANet	National Security Agency Network
NSC	National Security Council
NSS	national security system
NST	national support team

NSTISSC	National Security Telecommunications and Information Security Committee
NTSA	network traffic security analyzer
NWS	network warfare squadron
OC	operations center
OCO	offensive cyberspace operations
OCONUS	outside of continental United States
OGC	Office of General Counsel
OMB	Office of Management and Budget
ONE-NET	OCONUS Navy Enterprise Network
OPCON	operational control
OPORD	operation order
OPSEC	operations security
OT&E	organize, train, and equip
PACOM	United States Pacific Command
PAI	publicly available information
PCAP	packet capture
PII	personally identifiable information
POTUS	President of the United States
PPD	Presidential policy directive
QIA	questionable intelligence activity
RAT	remote access tool
RFA	request for assistance
SAD	State Active Duty
SAF/CN	Air Force Deputy Chief Information Officer
SAF/GCI	Office of the Secretary of the Air Force General Counsel

SAF/GCQ	Office of the Deputy General Counsel (Acquisition)
SCA	Stored Communications Act
SCC	Service cryptologic component
SECAF	Secretary of the Air Force
SecDef	Secretary of Defense
S/HSM	significant or highly sensitive matter
SIGINT	signals intelligence
SIPRNet	Secret Internet Protocol Router Network
SOCOM	United States Special Operations Command
SPACECOM	United States Space Command
STRATCOM	United States Strategic Command
TACON	tactical control
TAG	Adjutant General
TASKORD	tasking order
TCP/IP	Transmission Control Protocol/Internet Protocol
TEO	technology executive officer
TLD	top-level domain
TMA	traditional military action
TTP	tactics, techniques, and procedures
T2	technology transfer
UCP	Unified Command Plan
UN	United Nations
U.S.	United States
USAF	United States Air Force
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command
USG	United States Government
USN	United States Navy
USPI	United States person information
USSOUTHCOM	United States Southern Command
USTRANSCOM	United States Transportation Command
VCLT	Vienna Convention on the Law of Treaties
VPN	virtual private network

References

Table of Authorities

Statutory Authorities

10 U.S.C. §§ 161-167b.	Combatant commands: Establishment (§ 161); Assigned forces; chain of command (§ 162); Role of Chairman of Joint Chiefs of Staff (§ 163); Commanders of combatant commands: assignment; powers and duties (§164); Administration and support (§ 165); Budget proposals (§ 166); Funding through the Chairman of Joint Chiefs of Staff (§ 166a); Funding for combating terrorism readiness initiatives (§ 166b); Unified combatant command for special operations forces (§ 167); Unified combatant command for cyber operations (§ 167b) https://uscode.house.gov/
10 U.S.C. §§ 394-395.	Cyber and Information Operations Matters: Authorities concernin, military cyber operations (394); Notification requirements for sensitive military cyber operations (§ 395) https://uscode.house.gov/
10 U.S.C. § 923.	UCMJ, Art. 123: Offenses concerning Government computers https://uscode.house.gov/
10 U.S.C. § 7013	Department of the Army: Secretary of the Army https://uscode.house.gov/
10 U.S.C. § 9013.	Air Force Organization: Secretary of the Air Force https://uscode.house.gov/
15 U.S.C. § 3710.	Technology Innovation: Utilization of Federal technology https://uscode.house.gov/
17 U.S.C. § 1201.	Copyright Protection and Management Systems: Circumvention of copyright protection systems https://uscode.house.gov/

Statutory Authorities (*continued*)

18 U.S.C. § 641.	Embezzlement and Theft: Public money, property or records https://uscode.house.gov/
18 U.S.C. §§ 793-798.	Espionage and Censorship: Gathering, transmitting or losing defense information (§ 793); Gathering or delivering defense information to aid foreign government (§ 794); Photographing and sketching defense installations (§ 795); Use of aircraft for photographing defense installations (§ 796); Publication and sale of photographs of defense installations (§ 796); Disclosure of classified information (§ 798) https://uscode.house.gov/
18 U.S.C. §§ 1028-1030.	Fraud and False Statements: Fraud and related activity in connection with identification documents, authentication features, and information (§ 1028); Aggravated identity theft (§ 1028A); Fraud and related activity in connection with access devices (§ 1029); Fraud and related activity in connection with computers (§ 1030) https://uscode.house.gov/
18 U.S.C. § 1343.	Mail Fraud and Other Fraud Offenses: Fraud by wire, radio, or television https://uscode.house.gov/
18 U.S.C. § 1385.	Military and Navy: Use of Army, Navy, Marine Corps, Air Force, and Space Force as *posse comitatus* https://uscode.house.gov/
18 U.S.C. § 2511.	Wire and Electronic Communications Interception and Interception of Oral Communications: Interception and disclosure of wire, oral, or electronic communications prohibited https://uscode.house.gov/

Statutory Authorities (*continued*)

18 U.S.C. § 2701, § 2703, §2707, §2711(3)(c).	Stored Wire and Electronic Communications and Transactional Records Access: Unlawful access to stored communications (§ 2701); Required disclosure of customer communications or records (§ 2703); Civil action (§ 2707); Definitions (§ 2711[3][c]) https://uscode.house.gov/
18 U.S.C. § 3121, § 3127.	Pen Registers and Trap and Trace Devices: General prohibition on pen register and trap and trace device use; exception (§ 3121; Definitions for chapter (§ 3127) https://uscode.house.gov/
31 U.S.C. §§ 1535-1536.	Transfers and Reimbursements: Agency agreements (§ 1535); Crediting payments from purchases between executive agencies (§ 1536) https://uscode.house.gov/
31 U.S.C. §§ 6303-6305.	Using Procurement Contracts and Grant and Cooperative Agreements: Using procurement contracts (§ 6303); Using grant agreements (§ 6304); Using cooperative agreements (§ 6305) https://uscode.house.gov/
42 U.S.C. §§ 5121-5206.	Disaster Relief (Stafford Act) https://uscode.house.gov/
44 U.S.C. §§ 3601-3606.	Management and Promotion of Electronic Government Services: Definitions (§ 3601); Office of Electronic Government (§ 3602); Chief Information Officers Council (§ 3603); E-Government Fund (§ 3604); Program to encourage innovation solutions to enhance electronic Government services and processes (§ 3605); E-Government report (§ 3606) https://uscode.house.gov/

Statutory Authorities (*continued*)

44 U.S.C. §§ 3551-3552, 3554.	Information Security: Purposes (§ 3551); Definitions (§ 3552); Federal agency responsibilities (§ 3554) https://uscode.house.gov/
50 U.S.C. § 1541.	War Powers Resolution: Purpose and policy https://uscode.house.gov/
50 U.S.C. § 1801.	Electronic Surveillance: Definitions https://uscode.house.gov/
50 U.S.C. § 3091, § 3093.	Accountability for Intelligence Activities: General congressional oversight provisions (§ 3091); Presidential approval and reporting of covert actions (§ 3093) https://uscode.house.gov/

Clarifying Lawful Overseas Use of Data (CLOUD) Act. H.R. Res. 1625, 115th Cong. (2018). https://www.congress.gov/.

E-Government Act of 2002. Pub. L. 107-347. 116 Stat. 2899 (2002). https://www.congress.gov/.

Electronic Communications Privacy Act of 1986. Pub. L. No. 99-508 (1986). https://www.govinfo.gov/.

Federal Information Security Modernization Act of 2014. Pub L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/.

Goldwater-Nichols Department of Defense Reorganization Act of 1986. Pub. L. No. 99-433, 100 Stat. 992 (1986). https://www.govinfo.gov/.

Intelligence Reform and Terrorism Prevention Act 2004. Pub. L. No. 108-458. 188 Stat. 3638 (2004). https://www.govinfo.gov/.

John S. McCain National Defense Authorization Act for Fiscal Year 2019. Pub. L. No. 115-232, § 1642, 132 Stat. 1636, 2132 (2018). https://www.congress.gov/.

Knight First Amendment Institute v. Trump, 928 F.3d 226, 568-570 (2d. Cir. 2019) https://casetext.com/.

National Defense Authorization Act for Fiscal Year 2012. Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011). https://www.congress.gov/.

Statutory Authorities (*continued*)

National Defense Authorization Act for Fiscal Year 2018. Pub. L. No. 115-91, § 1637, 131 Stat. 1283, 1742 (2017), https://www.congress.gov/.

National Defense Authorization Act for Fiscal Year 2020. Pub. L. No. 116-92, § 1631, 133 Stat. 1198, 1741 (2019). https://www.govinfo.gov/.

National Security Act of 1947. Pub. L. No. 80-253, 61 Stat. 495 (1947). https://catalog.archives.gov/.

Robert T. Stafford Disaster Relief and Emergency Act. Pub. L. No. 100-707, 102 Stat. 4689 (1988). https://www.govinfo.gov/.

Regulatory Authorities

32 C.F.R. § 185.	*Reserved by* Defense Support of Civil Authorities, 83 Fed. Reg. 14589 (Apr. 5, 2018) (to be codified at 32 C.F.R. pt. 185). https://www.govinfo.gov/.
48 C.F.R. § 204.7300.	Scope (Defense Federal Acquisition Regulation Supplement [DFARS]). https://w8ww.govinfo.gov/.

Constitutional Authorities

U.S. Const. amends. I, IV, V. https://constitutioncenter.org/.

U.S. Const. art. 1, § 8. https://constitutioncenter.org/.

U.S. Const. art. II, §§ 1 and 2. https://constitutioncenter.org/.

Judicial Authorities

Carpenter v. United States, 138 S.Ct. 2206 (2018). https://www.supremecourt.gov/.

Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp. 333 U.S. 103, 111 (1947). https://supreme.justia.com/.

Corfu Channel (U.K. v. Alb.), Judgement, 1949 I.C.J. Rep. 4, 35 (Apr. 9, 1949). https://www.icj-cij.org/.

Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013). https://casetext.com/.

Judicial Authorities (*continued*)

Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010). https://www.leagle.com/.

Department of Justice. Cloud Act. Accessed December 2021. https://www.justice.gov/.

_____. *Criminal Resource Manual*, §§ 668, 670-671, and 1061, updated January 2020. https://www.justice.gov/.

_____. *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*. Washington, DC: Department of Justice, April 2019. https://www.justice.gov/.

Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068 (9th Cir. 2016). https://casetext.com/.

International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006). https://casetext.com/.

Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013). https://www.leagle.com/.

Kemp v. Block, 607 F. Supp. 1262 (D. Nev. 1985). https://www.courtlistener.com/.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). https://openjurist.org/.

Legal Status of Eastern Greenland (Denmark v. Norway), 1933 P.C.I.J. (ser. A/B) No. 53, at 71 (Apr. 5, 1933) (holding that a unilateral statement made on behalf of a country's government by its minister of foreign affairs may be binding on that country). https://jusmundi.com/.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment, 1986 I.C.J. [International Court of Justice] 14 (Jun. 27, 1986). https://www.icj-cij.org/.

Nardone v. United States, 302 U.S. at 383-84. https://supreme.justia.com/.

Nickelodeon Consumer Privacy Litig., No. 2443 (SRC), 2014 U.S. Dist. LEXIS 91286 (D.N.J. July 2, 2014). https://www.wsgr.com/.

Prize Cases, 67 U.S. (2 Black) 635 (1863). https://www.lexisnexis.com/.

Smith v. Maryland, 442 U.S. 735 (1979). https://supreme.justia.com/.

Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006). https://casetext.com/.

Sparshott v. Feld Entertainment, Inc., 354 U.S. App. D.C. 63, 311 F.3d 425 (2002). https://casetext.com/.

Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003). https://casetext.com/.

Judicial Authorities (*continued*)

Totten v. United States, 92 U.S. 105, 106 (1876). https://casetext.com/.

United States for Orders Authorizing Installation and Use of Pen Registers, 416 F. Supp. 2d 13 (D.D.C. 2006). https://cite.case.law/.

United States of Am. for an Order Authorizing the Installation and Use of a Pen Register, 402 F. Supp. 2d 597 (D. Md. 2005). https://casetext.com/.

United States v. Cotroni, 527 F.2d 708 (2d Cir. 1975). https://www.courtlistener.com/.

United States v. Councilman, 418 F.3d 67 (1st Cir. 2005). https://openjurist.org/.

United States v. Curtiss-Wright Corp, 299 U.S. 304, 320 (1936). https://supreme.justia.com/.

United States v. Dunbar, 553 F.3d 48 (1st Cir. 2009). https://www.courtlistener.com/.

United States v. John, 597 F.3d 263, 271-73 (5th Cir. 2010). https://casetext.com/.

United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992). https://casetext.com/.

United States v. Larson, 66 M.J. 212 (C.A.A.F. 2008). https://cases.justia.com/.

United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017). https://www.armfor.uscourts.gov/.

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). https://casetext.com/.

United States v. Nosal, 828 F.3d 865 (9th Cir. 2016). https://casetext.com/.

United States v. Robinson, 77 M.J. 303 (C.A.A.F. 2018). https://www.armfor.uscourts.gov/.

United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010). https://casetext.com/.

United States v. Valle, 807 F.3d 508 (2nd Cir. 2015). https://casetext.com/.

United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019). https://www.law.cornell.edu/.

Van Buren v. United States, No. 19-783, 2020 WL 1906566 (U.S. Apr. 20, 2020) (argued Nov. 30, 2020). https://www.supremecourt.gov/.

Van Buren v. United States, 141 S. Ct. 1648 (2021). https://www.lexisnexis.com/.

WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012). https://casetext.com/.

Judicial Authorities (*continued*)

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952). https://supreme.justia.com/.

Executive Authorities

Biden, Joseph. Interim National Security Strategic Guidance. Washington, D.C.: White House, March 2021. https://www.whitehouse.gov/.

Exec. Order No. 12333. United States Intelligence Activities, December 4, 1981. https://www.archives.gov/.

Exec. Order No. 12968. Access to Classified Information, 60 Fed. Reg. 40,425 (1995). https://www.govinfo.gov/.

Exec. Order No. 13231. Critical Infrastructure Protection in the Information Age, October 16, 2001. https://www.govinfo.gov/.

Exec. Order No. 13549. Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, 75 Fed. Reg. 51,609 (2010). https://www.federalregister.gov/.

Presidential Policy Directive 8 (PPD-8). National Preparedness, March 30, 2011. https://www.dhs.gov/.

Presidential Policy Directive 41 (PPD-41). United States Cyber Incident Coordination, July 26, 2016. https://www.whitehouse.gov/.

Air Force / Department of the Air Force Instructions and Directives

Department of the Air Force instructions (DAFI) apply to the U.S. Air Force (USAF) and U.S. Space Force (USSF) while Air Force instructions (AFI) apply only to the U.S. Air Force. As publications are revised or established, they will specifically refer to the USAF, USSF, or DAF.

Air Force Instruction (AFI) 10-701. *Operations Security*, July 24, 2019 (inc. C1, June 9, 2020). https://static.e-publishing.af.mil/.

AFI 17-101. *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, February 6, 2020. https://static.e-publishing.af.mil/.

AFI 33-332. *Air Force Privacy and Civil Liberties Program*, March 10, 2020 (inc. C1, May 12, 2020). https://static.e-publishing.af.mil/.

AFI 51-401. *The Law of War*, August 3, 2018. https://static.e-publishing.af.mil/.

Air Force / Department of the Air Force Instructions and Directives
(*continued*)

AFI 61-301. *The Domestic Technology Transfer Process and the Offices of Research and Technology Applications Cooperative Research and Development Agreements*, September 16, 2019. https://irp.fas.org/.

AFI 71-101V4. *Counterintelligence*, July 2, 2019. https://irp.fas.org/.

Air Combat Command. "Cyber Command and Control Mission System (C3MS)." Fact sheet, January 24, 2020. https://www.acc.af.mil/.

Air Combat Command Instruction (ACCI)10-810. *Operations Involving Domestic Imagery Support (ISR/OPSRECCE/RPA) Request Procedures for US Missions*, December 17, 2013. https://www.hsdl.org/.

Air Combat Command Manual (ACCMAN) 14-402. *Unit-Level Intelligence Mission and Responsibilities*, March 25, 2020. https://static.e-publishing.af.mil/.

Air Force Manual (AFMAN) 14-405. *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, May 11, 2020. https://static.e-publishing.af.mil/.

Air Force Manual (AFMAN) 17-1301. *Computer Security (COMPUSEC)*, February 12, 2020. https://static.e-publishing.af.mil/.

Department of the Air Force Instruction (DAFI) 17-130. *Cybersecurity Program Management*, February 13, 2020. https://static.e-publishing.af.mil/.

Department of the Air Force Instruction (DAFI) 17-201. *Command and Control (C2) for Cyberspace Operations*, March 5, 2014, with Air Force Guidance Memorandum 2016-1, May 12, 2016. https://irp.fas.org/.

Department of the Air Force Policy Directive (DAFPD) 17-2. *Cyber Warfare Operations*, October 27, 2020. https://static.e-publishing.af.mil/.

Department of the Air Force. *The United States Air Force Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy*. Washington, DC: Department of the Air Force, 2019. https://www.af.mil/.

_____. 2018 CJCS Defense Support of Civil Authorities EXORD, June 5, 2018.

Headquarters Air Force Mission Directive (HAFMD) 1-33. *Deputy Chief of Staff of the Air Force, Intelligence, Surveillance, and Reconnaissance*, September 18, 2015. https://static.e-publishing.af.mil/.

Air Force / Department of the Air Force Instructions and Directives (*continued*)

Headquarters Air Force. Program Guidance Letter (PGL) 18-22. T*ransfer of cyberspace lead command, cyberspace superiority core function lead, and cyberspace operations responsibilities from Air Force Space Command to Air Combat Command*, February 8, 2018.

_____. Program Guidance Letter (PGL) 19-05. *Establishment of the Information Warfare (IW) Component Numbered Air Force (C-NAF) under Air Combat Command*, September 6, 2019.

The Judge Advocate General's (JAG) School. *The Law of Air, Space, and Cyber Operations*. 4th ed. Maxwell AFB, AL: JAG School, 2020. https://www.afjag.af.mil/.

Department of Defense and Joint Staff Directives, Instructions, and Publications

Chairman of the Joint Chiefs of Staff Guide (CJCS) 3130. *Adaptive Planning and Execution Overview and Policy Framework*, March 5, 2019. https://www.jcs.mil/.

Defense Information Systems Agency (DISA). "Enterprise Mission Assurance Support Service (eMASS)." Fact sheet. Accessed January 10, 2022. https://www.disa.mil/.

Department of Defense, Office of General Counsel. *Department of Defense Law of War Manual*. Washington, D.C.: Office of General Counsel, Department of Defense, June 2015 (updated December 2016). https://dod.defense.gov/.

Department of Defense Directive 2311.01. *DoD Law of War Program*, July 2, 2020. https://www.esd.whs.mil/.

Department of Defense Directive 3000.03E. *DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, April 25, 2013 (inc. C2, August 31, 2018). https://www.esd.whs.mil/.

Department of Defense Directive 3020.40. *Mission Assurance (MA)*, November 29, 2016. https://www.esd.whs.mil/.

Department of Defense Directive 3025.18. *Defense Support of Civil Authorities (DSCA)* (inc. C 2, March 19, 2018). https://www.esd.whs.mil/.

Department of Defense Directive 3115.18. *DoD Access to and Use of Publicly Available Information (PAI)*, July 11, 2019 (inc. C1, August 20, 2020). https://irp.fas.org/.

Department of Defense and Joint Staff Directives, Instructions, and Publications (*continued*)

Department of Defense Directive 3600.01. *Information Operations (IO)*, May 2, 2013 (inc. C1, May 4, 2017). https://www.esd.whs.mil/.

Department of Defense Directive 5000.01. *The Defense Acquisition System*, September 9, 2020. https://www.esd.whs.mil/.

Department of Defense Directive 5100.20. *National Security Agency/Central Security Service (NSA/CSS)*, January 26, 2010. https://www.esd.whs.mil/.

Department of Defense Directive 5105.19. *Defense Information Systems Agency (DISA)*, July 25, 2006. https://www.esd.whs.mil/.

Department of Defense Directive 5105.21. *Defense Intelligence Agency (DIA)*, March 18, 2008. https://www.esd.whs.mil/.

Department of Defense Directive 5148.13. *Intelligence Oversight*, April 26, 2017. https://dodsioo.defense.gov/.

Department of Defense Directive 5240.01. *DoD Intelligence Activities*, August 27, 2007 (inc. Change 3, November 9, 2020). https://www.esd.whs.mil/.

Department of Defense Instruction 5535.8. *DoD Technology Transfer (T2) Program*, May 14, 1999 (inc. C1, September 1, 2018). https://www.esd.whs.mil/.

Department of Defense Instruction 8010.01. *Department of Defense Information Network (DODIN) Transport*, September 10, 2018. https://www.esd.whs.mil/.

Department of Defense Instruction 8410.01. *Internet Domain Name and Internet Protocol Address Space Use and Approval*, December 4, 2015 (inc. C1, June 4, 2021). https://www.esd.whs.mil/.

Department of Defense Instruction 8510.01. *Risk Management Framework for DoD Information Technology (IT)*, March 12, 2014 (inc. C3, December 29, 2020). https://www.esd.whs.mil/.

Department of Defense Instruction 8530.01. *Cybersecurity Activities Support to DoD Information Network Operations*, March 7, 2016 (inc. C1, July 25, 2017). https://www.esd.whs.mil/.

Department of Defense Manual (DODM) 5240.01. *Procedures Governing the Conduct of DoD Intelligence Activities*, August 8, 2016. https://dodsioo.defense.gov/.

Department of Defense and Joint Staff Directives, Instructions, and Publications (*continued*)

Department of Defense Regulation 5240.01-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*, December 1982. https://www.esd.whs.mil/.

Department of Defense Regulation 7000.14-R. *Financial Management Regulation. Vol. 11A, Reimbursable Operations Policy*, September 2019. https://comptroller.defense.gov/.

Department of Defense *Software Modernization Strategy*. Version 1.0. Washington, DC: Department of Defense, November 2021. https://media.defense.gov/.

Department of Defense. *Summary: Department of Defense Cyber Strategy*. Washington, D.C.: DOD, September 2018. https://media.defense.gov/.

_____. *Summary of the 2018 Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity*. Washington, DC: Department of Defense, 2018. https://media.defense.gov/.

Deputy Secretary of Defense. To chief management officer of the Department of Defense et al. Memorandum. Subject: Establishment of the Joint Artificial Intelligence Center, June 27, 2018. https://admin.govexec.com/.

Directive-Type Memorandum (DTM) 17-007. "Interim Policy and Guidance for Defense Support to Cyber Incident Response," June 21, 2017 (inc. Change 4, May 21, 2021). https://www.esd.whs.mil/.

Joint Publication 3-12. *Cyberspace Operations*, June 8, 2018. https://www.jcs.mil/.

Joint Publication 3-28. *Defense Support of Civil Authorities*, October 29, 2018. https://www.jcs.mil/.

Office of the Chairman of the Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*. Washington, D.C.: The Joint Staff, November 2021. https://www.jcs.mil/.

Secretary of Defense, Chief Information Officer. "Cyber Squadron Enabling Concept," March 15, 2018.

Secretary of Defense to Chief Management Officer, Department of Defense et al. Memorandum. Subject: Definition of "Department of Defense Cyberspace Operations Forces (DoD COF)," December 12, 2019.

Other References

Berger, Joseph B., III. "Covert Action: Title 10, Title 50, and the Chain of Command." *Joint Force Quarterly* 67, no. 4 (October 2012): 32–39. https://ndupress.ndu.edu/.

Biller, Jeffrey. "The Misuse of Protected Indicators in Cyberspace: Defending a Core Aspect of International Humanitarian Law." *2017 9th International Conference on Cyber Conflict (CyCon)*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence [CCD COE] Publications, 2017. https://ccdcoe.org/.

British Institute of International and Comparative Law (BIICL). *State Responsibility for Cyber Operations: International Law Issues*. Event Report. London: BIICL, October 9, 2014. https://www.biicl.org/.

Charter of the United Nations, June 26, 1945, 59 Stat. 1031, at art. 2, para. 4. https://www.un.org/.

Chesney, Robert. "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate." J*ournal of National Security Law & Policy* 5 (2012): 539–629. https://jnslp.com/.

Committee on National Security Systems Instruction (CNSSI) No. 4009. *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015. https://rmf.org/.

Corn, Gary. "Tallinn Manual 2.0—Advancing the Conversation." Just Security, February 16, 2016. https://www.justsecurity.org/.

Corn, Gary, and Robert Taylor. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111 (2017): 207–12. https://doi.org/10.1017/aju.2017.57.

Deeks, Ashley. "Defend Forward and Cyber Countermeasures." *Lawfare*, August 12, 2020. https://www.lawfareblog.com/.

"Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, 2001. Brussels: United Nations, 2008. https://legal.un.org/. Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10). The report appears in the *Yearbook of the International Law Commission*, 2001. Vol. 2, pt. 2. New York; Geneva: United Nations, 2007. As corrected.

Goldfoot, Josh, and Aditya Bamzai. "A Trespass Framework for the Crime of Hacking." *George Washington Law Review* 84, no. 6 (2014): 1478–99. https://www.law.virginia.edu/.

Other References (*continued*)

Government Accountability Office (GAO). *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*. GAO-19-362. Washington, DC: GAO, March 2019. https://www.gao.gov/.

_____. *Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*. GAO-21-179. Washington, D.C.: GAO, March 4, 2021. https://www.gao.gov/.

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

International and Operational Law Department, The Judge Advocate General's Legal Center and School, U.S. Army. *Operational Law Handbook*. Charlottesville, VA: International and Operational Law Department, The Judge Advocate General's Legal Center and School, US Army, 2021. https://tjaglcs.army.mil/.

Kent, Suzette, U.S. Federal Chief Information Officer. *Federal Cloud Computing Strategy*. Washington, D.C.: Executive Office of the President of the United States, June 24, 2019. https://cloud.cio.gov/.

Kitfield, James A. "A Better Way to Run a War." *Air Force Magazine*, October 1, 2006. https://www.airforcemag.com/.

Koh, Harold Hongju, Legal Advisor, Department of State. "The Obama Administration and International Law." Address. Annual Meeting of the American Society of International Law, March 25, 2010. https://2009-2017.state.gov/.

Mačák, Kubo. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." *Israel Law Review* 48, no. 1 (2015): 55–80. https://doi.org/10.1017/S0021223714000260.

"Military Objectives." Cyber Law Toolkit. Accessed April 13, 2022. https://cyberlaw.ccdcoe.org/.

Office of Management and Budget (OMB) Circular No. A-130. Subject: Managing Information as a Strategic Resource, July 28, 2016. https://obamawhitehouse.archives.gov/.

Office of the Director of National Intelligence. *Intelligence Community Legal Reference Book*. Washington, DC: Office of the Director of National Intelligence, Office of General Counsel, Winter 2020. https://www.dni.gov/.

_____. "Members of the IC [Intelligence Community]." Accessed May 14, 2021. https://www.dni.gov/.

Other References (*continued*)

Ney, Hon. Paul C., Jr. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," March 2, 2020. https://www.defense.gov/.

"Perfidy and Ruses of War." Cyber Law Toolkit. Accessed January 5, 2022. https://cyberlaw.ccdcoe.org/.

Pilloud, Claude, Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC 1987). Edited by Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann. Geneva: Martinus Nijhoff Publishers, 1987. https://www.loc.gov/.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 8 June 1977. https://www.un.org/.

Schmitt, Michael N., and Liis Vihul, eds. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge, UK: Cambridge University Press, 2017.

Schmitt, Michael N., and Liis Vihul. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111 (2017): 213–18. https://doi.org/10.1017/aju.2017.55.

Schmitt, Michael N., gen. ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press, 2013. For a draft copy, see http://csef.ru/.

Skinner, Brig Gen Robert J. "The Importance of Designating Cyberspace Weapon Systems." *Air & Space Power Journal* 27, no. 5 (September–October 2013): 29–48. https://www.airuniversity.af.edu/.

Stevens, Gina, and Charles Doyle. *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*. Washington, DC: Congressional Research Service, October 9, 2012.

Theohary, Catherine A. *Defense Primer: Cyberspace Operations*. In Focus. Washington, D.C.: Congressional Research Service, December 1, 2021. https://crsreports.congress.gov/

Tsagourias, Nicholas. "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace." EJIL:Talk! (blog). *European Journal of International Law*, August 29, 2019. https://www.ejiltalk.org/.

Other References (*continued*)

United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397. https://www.un.org/.

U.S. Army Cyber Command. "DoD Fact Sheet: Cyber Mission Force," February 10, 2020. https://www.arcyber.army.mil/.

U.S. Cyber Command. "Cyber Mission Force Achieves Full Operational Capability." Press release, May 17, 2018. https://www.defense.gov/.

_____. "DOD Has Enduring Role in Election Defense," February 10, 2020. https://www.defense.gov/.

_____. "Our History." Accessed July 21, 2020. https://www.cybercom.mil/.

U.S. Department of Commerce, National Institute of Standards and Technology (NIST). Special Publication 800-53. *Security and Privacy Controls for Federal Information Systems and Organizations*. Rev. 5, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

_____. Special Publication 800-81-2. *Secure Domain Name System (DNS) Deployment Guide*, September 2013. https://nvlpubs.nist.gov/.

_____. Special Publication 800-128. *Guide for Security-Focused Configuration Management of Information Systems*, August 2011 (last updated October 10, 2019). https://nvlpubs.nist.gov/.

_____. Special Publication 800-145. *The NIST Definition of Cloud Computing*, September 2011. https://nvlpubs.nist.gov/.

U.S. Space Command. "Organizational Fact Sheet," June 20, 2018. https://www.spacecom.mil/.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *National Security Journal* 3, no. 1 (2011): 85–142. https://harvardnsj.org/.

Whitaker, Richard M. "Intelligence Law." In *U.S. Military Operations: Law, Policy, and Practice*, edited by Geoffrey S. Corn, Rachel E. VanLandingham, and Shane R. Reeves. New York: Oxford University Press, 2015.

Yoo, John. "The Legality of the National Security Agency's Bulk Data Surveillance Programs." *I/S: A Journal of Law and Policy for the Information Society* 10, no. 2 (2014): 301–26. https://kb.osu.edu/.

Zoldi, Dawn M. K. "Protecting Security and Privacy: An Analytical Framework for Airborne Domestic Imagery." *Air Force Law Review* 70 (2013): 1–30. https://www.afjag.af.mil/.

AIR UNIVERSITY PRESS

http://www.au.af.mil/au/aupress/

ISSN 2831-5251