Congressional Research Service
Informing the legislative debate since 1914

Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions

Updated November 29, 2022

Congressional Research Service
https://crsreports.congress.gov
R45175

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45175

November 29, 2022

Michael E. DeVine
Analyst in Intelligence and National Security

Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions

Congress has defined in statute several definitions of covert action and clandestine activities carried out by the Intelligence Community (IC); other definitions appear only in committee reports and still others are military terms. These definitions describe activities that support U.S. national security policy, and are, therefore, important to Congress's intelligence and defense oversight responsibilities.

Uncertainty over the proper jurisdiction for congressional oversight can occur, however, when covert action or clandestine intelligence activities appear similar to certain military operations that may employ clandestine methodology or have objectives similar to those for covert action. Intelligence and military matters fall under different authorities of the *U.S. Code*, and have, as a result, different statutory requirements for providing notification to Congress. Applicable statutes that govern intelligence activities under Title 50 of the *U.S. Code* emphasize *prior* notification to the congressional intelligence committees for each separate activity. Under its Title 10 *U.S. Code* authorities, however, the Department of Defense (DOD) generally provides notification of certain types of secret or clandestine military operations to the Armed Services committees *after* their commencement, often by briefing Congress as part of a larger, supported military operation or campaign.

The IC, for example, in conducting a covert action, must generally provide prior notification to the congressional intelligence committees by means of a presidential finding describing plans to have an intelligence operation influence political, military, or economic conditions abroad while concealing U.S. sponsorship. The military, on the other hand, under Title 10, has the implicit authority to conduct operations that resemble covert action, but which DOD classifies as traditional military activities or operational preparation of the environment. These activities are handled differently for oversight purposes, despite sharing with covert actions conducted under Title 50 authorities a number of characteristics that heighten Congress's interest: a serious risk of exposure of U.S. involvement, compromise of information, or loss of life.

Congress has attempted to settle the challenges over which committees exercise oversight by defining the terms for selected intelligence and military activities in statute as either covert action or exceptions to covert action. The congressional intelligence committees exercise oversight jurisdiction over covert action, which is defined under Title 50 as an activity or activities of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will *not* be apparent or acknowledged publicly. This definition has exceptions, including, for example, activities involving intelligence collection, counterintelligence, law enforcement, and—significantly—traditional military activities. Traditional military activities are all the types of activities, conducted under Title 10 authority, which take place under a military chain of command as part of an ongoing or anticipated conflict in which the overall role of the United States is publicly acknowledged. Although most are overt and conventional, traditional military activities can be conducted clandestinely in which case the activity itself as well as the role of the United States is secret. The congressional armed services committees exercise oversight jurisdiction over traditional military activities regardless of how secret or sensitive they may be. An understanding of how these and related terms are used can help Congress navigate potential challenges in conducting oversight.

Contents

Contacts

Introduction

This report provides background and definitions for covert action and clandestine activities carried out by the Intelligence Community (IC) and military. It is the first of three reports on covert action and clandestine activities of the IC. The second, CRS Report R45191, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements in Brief*, by Michael E. DeVine, describes the different statutory requirements for keeping Congress informed of these activities. The third, CRS Report R45196, *Covert Action and Clandestine Activities of the Intelligence Community: Framework for Congressional Oversight In Brief*, by Michael E. DeVine, is intended to assist Congress in assessing the premises justifying covert action and clandestine activities, their impact on national security, operational viability, funding requirements, and possible long-term or unintended consequences.

Congressional oversight of the Intelligence Community enables Members of Congress to gain insight into and offer advice on programs and activities that can significantly influence U.S. foreign policy and its outcomes.[1] This report addresses Congress's ongoing interest in oversight of covert action and clandestine operations.

The distinction between government agency activities described as *covert* and *clandestine* can sometimes raise uncertainties and involve consideration of several factors. Which agencies are authorized to conduct covert action and clandestine activities? What are their legal authorities for doing so? Which military terms describe activities that might seem similar but are distinct from covert action?

Covert action is defined in statute as an activity or activities of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will *not* be apparent or acknowledged publicly.[2] The statutory definition of covert action also specifies that it does not include traditional military activities, traditional intelligence collection or counterintelligence activities, or traditional law enforcement activities.[3]

While not defined in statute, Department of Defense (DOD) doctrine describes a clandestine operation as "an operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment."[4] Clandestine operations often involve relatively passive intelligence collection operations. Unlike covert action, clandestine activities do not require prior notice to Congress via a presidential *finding,* but may still require notification of Congress.[5] Under the DOD definition, *clandestine differs* from *covert* as it typically involves

[1] The IC is a federation of 18 elements spread across two independent agencies and six separate departments of the federal government. Many IC elements reside within the DOD organizational structure, including the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), the National Security Agency (NSA), and the intelligence components of the military service branches. For more on the IC, see CRS In Focus IF10525, *Defense Primer: National and Defense Intelligence*, by Michael E. DeVine, as well as P.L. 108-458 (the Intelligence Reform and Terrorism Prevention Act of 2004, also known as IRTPA) and Executive Order 12333, as amended. See also Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal*, vol. 3, no. 1 (2011): 85-142.

[2] 50 U.S.C. §3093(e).

[3] 50 U.S.C. §3093(e)(1)-(3).

[4] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms,* November 2021, p. 35, at https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.

[5] 50 U.S.C. §3093(a) describes a finding as a written presidential authorization for a specific department or agency to conduct a specified covert action that the President determines is necessary to support "identifiable foreign policy

concealment of a tactical activity. By comparison, covert operations are "planned and executed to conceal the identity of, or permit plausible deniability by, the sponsor."[6]

Background

Congress established a statutory framework for conducting oversight of intelligence activities in the mid-1970s.

Prior to 1974, Congress exercised what some have described as "benign neglect" of intelligence activities.[7] Congress did not question whether particular covert actions or other sensitive intelligence activities were viable or ethical as a means of supporting U.S. national security. In 1953, for example, when President Dwight D. Eisenhower authorized the Central Intelligence Agency (CIA) to orchestrate the overthrow of Iran's democratically elected government, there was no dedicated congressional intelligence oversight framework, nor was there any statutory requirement for the President to inform Congress of such activities.

In the 1970s, public controversy over the disclosure of the CIA's covert action programs in Southeast Asia and the agency's domestic surveillance of Vietnam War-era antiwar movement activists spurred Congress to become more involved in intelligence oversight.[8] The Hughes-Ryan amendment of the Foreign Assistance Act of 1961 (§32 of P.L. 93-559, signed by President Gerald R. Ford on December 30, 1974), provided the first statutory basis for notification of Congress and congressional oversight of covert action operations. The Hughes-Ryan Amendment allowed appropriated funds to be spent on a covert action only after the President issued a *finding* which included a description of the nature and scope of the activity which the president found to be important to U.S. national security.

Congress's growing interest in intelligence activities led to investigations in 1975 by two congressional select committees: in the Senate, chaired by Senator Frank Church, and in the House, chaired by Representative Otis Pike.[9] Their work provided the first formal effort to understand the scope of past intelligence activities. These committees became the model for a permanent oversight framework that could hold the IC accountable for spending appropriated funds ethically, legally, and on programs and activities that supported identifiable national security objectives. In 1976, Congress established the Senate Select Committee on Intelligence (SSCI), followed by the House Permanent Select Committee on Intelligence (HPSCI) in 1977.

Congress subsequently refined its oversight provisions governing covert action in response to two incidents when the President chose not to inform Congress in advance of an operation. In August 1980, out of concern for maintaining operational security, President Jimmy Carter chose not to inform Congress prior to the attempt to rescue American hostages held by the Iranian regime. In

objectives" which are important to the national security of the United States."

[6] Ibid, p. 53.

[7] James S. Van Wagenen, *A Review of Congressional Oversight: Critics and Defenders* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2007), at https://www.cia.gov/static/505598ba08c99a3e1fbaed7d745cb054/Review-of-Congressional-Oversight.pdf.

[8] Seymour Hersh's disclosure in the *New York Times* of CIA activities was instrumental in generating public interest in U.S. intelligence activities at home and abroad. See Seymour Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times*, December 22, 1974, at https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html.

[9] In the Senate the Church committee was formally called the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Its House counterpart, the Pike committee, was known as the United States House Permanent Select Committee on Intelligence.

the mid-1980s, the Reagan Administration did not inform Congress about a covert initiative to divert funds raised from the sale of arms to Iran to support the Contras in Nicaragua. Through the Intelligence Authorization Acts (IAA) of 1981 (P.L. 96-450) and 1991 (P.L. 102-88), Congress revised procedures to require the executive branch to provide timely, comprehensive notification of all covert action and other "significant anticipated intelligence activity."[10]

While the jurisdiction of the SSCI and HPSCI for oversight of intelligence matters differed from the congressional armed services committees' jurisdiction over military matters, the evolution of U.S. counterterrorism operations abroad after the terrorist attacks of September 11, 2001 (hereinafter, "9/11") has sometimes made it difficult to distinguish between intelligence and military activities.[11] From an operational standpoint, this development was efficient: It sought to increase the overall effectiveness of counterterrorism operations in the field by integrating intelligence activities with the military's operations. From the standpoint of congressional oversight, however, it posed particular challenges. A counterterrorist operation involving components of the IC and military might be of interest to both the congressional armed services and intelligence committees. However, there are different notification standards and processes for keeping Congress informed, depending upon both how the IC or military categorize the activity, and whether it falls under the oversight jurisdiction of the congressional intelligence or armed services committees. Intelligence and military activities are governed by their respective statutory authorities: Title 50 of the *U.S. Code* provides the statutory authority for intelligence activities carried out in support of national requirements, even those by agencies within DOD. Title 10 of the *U.S. Code* provides the statutory authority for military operations, which usually include intelligence activities in direct support of these operations.

These separate authorities may give the impression that intelligence activities are separate and distinct from military operations. Yet, it is often the case that these activities and operations are mutually inclusive. Thus, from an oversight perspective, the congressional intelligence and armed services committees may consider overlapping matters. For example, intelligence activities and military operations can have a similar impact on national security and foreign relations because they may have common objectives, employ related methodologies, and share risks of the loss of life.

Congress has worked to resolve issues of committee jurisdiction by defining key terms in statute. These terms include covert actions, which are executed under Title 50 authority and fall under the oversight jurisdiction of the congressional intelligence committees, as well as the statutory exclusions from covert action which include the broad scope of different activities that constitute what is described in statute as traditional military activities and fall under the oversight jurisdiction of the congressional defense committees.

The following sections explain the distinctions between Title 10 and Title 50 authorities, and provide definitions of the intelligence activities and military operations that are sometimes difficult to distinguish, yet are subject to distinct congressional oversight.

---

[10] See Intelligence Authorization Act for FY1991, Title VI, §1325 (S. 1325, 102nd Congress); and Intelligence Authorization Act for 1981, at https://www.gpo.gov/fdsys/pkg/STATUTE-94/pdf/STATUTE-94-Pg1975.pdf). Specifications of "significant anticipated intelligence activities" and "significant intelligence failures" other than covert action that are reportable to Congress can be found in Intelligence Directive 112, *Congressional Notification*, June 29, 2017, at https://www.dni.gov/files/documents/71017/6-29-17_ICD-112_17-00383_U_SIGNED.PDF.

[11] The four congressional defense committees include the Armed Services and Appropriations committees of the Senate and House of Representatives. See 10 U.S.C. §101(a)(16). One member from each of the House defense committees also is a member of the HPSCI. One member from each party from each of the Senate defense committees is also a member of the SSCI.

Comparing Title 10 and Title 50 Authorities

Understanding the different statutory authorities for the intelligence activities and military operations defined in this report can aid in understanding how these activities are categorized, how Congress is notified, and which congressional committees have oversight jurisdiction. The *United States Code*, the compilation of codified United States federal statutes, is organized into *titles* by subject matter.[12] Title 10 of the *U.S. Code* provides much of the legal framework—sometimes referred to as *authorities*—for the roles, missions, and organization of DOD and the military services. Title 50 provides much of the legal framework for many of the roles and responsibilities of the IC, including the operations and functions of the CIA, as well as the legal requirements and congressional notification procedures associated with covert action.

Observers and practitioners may refer to *Title 10* and *Title 50 authorities* to signify

- executive decision making processes,
- congressional oversight structures,
- chains of command,
- legal authorizations to carry out certain types of activities,
- funding sources, and
- legal constraints preventing certain types of activities that govern the respective operations and activities of DOD and the IC.[13]

Legal observers, however, have pointed to the occasional difficulty in drawing clear distinctions between activities conducted under Title 10 authority and activities conducted under Title 50 authority. Some, therefore, assert that Title 10 and Title 50 authorities should instead be viewed as "mutually supporting" rather than "mutually exclusive" authorities.[14] Others further emphasize that Title 10 is not the sole source of legal authority for U.S. military operations, pointing to the President's authority under Article II of the Constitution as Commander in Chief of the U.S. Armed Forces, as well as laws enacted by Congress, such as the War Powers Resolution of 1973 (P.L. 93-148; 50 U.S.C. §1541-1548) and the 2001 Authorization for Use of Military Force (P.L. 107-40; 50 U.S.C. §1541 note).[15] Some also cite the dual role of the Secretary of Defense under Title 10 and Title 50 to exercise authority, direction, and control over those elements of the IC that reside within the DOD organizational structure as support for the argument that Title 10 and Title 50 should be viewed as "mutually supporting."[16]

---

[12] For a discussion of the organization and contents of the U.S. Code, see U.S. House of Representatives, Office of the Law Revision Counsel, "Detailed Guide to the United States Code Content and Features," available at http://uscode.house.gov/detailed_guide.xhtml.

[13] Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate." *Journal of National Security Law & Policy* vol. 5, no. 2 (2012): p. 615-616; see also Joshua Kuyers, "'Operational Preparation of the Environment: 'Intelligence Activity' or 'Covert Action' by Any Other Name?" *American University National Security Law Brief*, vol. 4, no. 1 (2013): 21-40.

[14] See Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal*, vol. 3, no. 1 (2011), p. 85, at https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.

[15] See CRS In Focus IF10534, *Defense Primer: President's Constitutional Authority with Regard to the Armed Forces*, by Jennifer K. Elsea, and CRS In Focus IF10535, *Defense Primer: Congress's Constitutional Authority with Regard to the Armed Forces*, by Jennifer K. Elsea. See also CRS Report R42699, *The War Powers Resolution: Concepts and Practice*, by Matthew C. Weed. See also Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate." *Journal of National Security Law & Policy*, vol. 5, no. 2 (2012): pp. 615-616.

[16] Andru E. Wall, pp. 85-142.

Selected Terms, Definitions, and Descriptions

Covert Action

Covert action is defined in Title 50 of the *U.S. Code* as an activity or activities of the U.S. government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will *not* be apparent or acknowledged publicly. It does not include

- activities with the primary purpose of acquiring intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of U.S. government programs, or administrative activities;
- traditional military or diplomatic activities or routine support to such activities;
- traditional law enforcement activities conducted by U.S. government law enforcement agencies or routine support to such activities;
- activities to provide routine support of any other overt activities of other U.S. government agencies abroad.[17]

Covert action is generally intended to strategically influence a targeted environment overseas without a sizable or extended military commitment.[18] Unlike most traditional intelligence collection, covert action is not passive. It has a visible, public impact intended to influence a change in the military, economic, or political environment abroad that might otherwise prove counterproductive if the role of the United States were made known.[19]

Covert action also requires a *finding* by the President, providing written notification to Congress that the impending activity supports "identifiable foreign policy objectives."[20] Covert action cannot be directed at influencing the U.S. domestic environment: "No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media."[21] While covert action is historically most closely associated with the CIA, the President may authorize other "departments, agencies or entities of the United States Government," such as DOD, to conduct covert action.[22]

Known historic examples of covert action include the CIA's orchestration of the 1953 coup in Iran; the 1961 Bay of Pigs invasion of Cuba; the Vietnam-era secret war in Laos; support to both

[17] See 50 U.S.C. §3093(e).

[18] "[T]here are areas of the world where a little covert action can forestall much more serious problems later." William Colby, late Director of the CIA. Randall B. Woods, *Shadow Warrior: William Egan Colby and the CIA*, (New York: Basic Books, 2013), p. 472.

[19] The late Director of the CIA, William Colby, once observed that it should be assumed the U.S. role in a covert action will become public knowledge at some point. See Mark M. Lowenthal, *Intelligence: From Secrets to Public Policy*, 7th ed. (Los Angeles: CQ Press, 2017), p. 251.

[20] 50 U.S.C. §3093(a).

[21] Ibid., §3093(f).

[22] Ibid., §3093(a)(3), "Each finding shall specify *each department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action*. Any employee, contractor, or contract agent of a department, agency, or entity of the United States Government other than the Central Intelligence Agency directed to participate in any way in a covert action shall be subject *either* to the policies and regulations of the Central Intelligence Agency, *or to written policies or regulations adopted by such department, agency, or entity, to govern such participation*." [emphasis added]

the Polish Solidarity labor union in the 1970s and 1980s; and support to the Mujahidin in Afghanistan during the 1980s. A number of these examples took place prior to the statutory requirement for issuing a presidential *finding* and highlight the mixed record and often unforeseen consequences of covert action historically. The 2011 raid on Osama bin Laden's compound is another example of what publicly has been acknowledged to have been a covert action.[23] Offensive cyberspace operations—defined as operations "intended to project power by the application of force in and through cyberspace"—may be classified as covert action only if they are accompanied by a presidential finding and conducted under authority of Title 50 of the *U.S. Code*, Section 3093, which provides the statutory provisions for oversight of covert action.[24]

Other-than-Routine Support to Traditional Military Activities

Only the SSCI has definitively categorized *other-than-routine support* to military operations as a type of covert action that includes a range of activities in which the U.S. role is unacknowledged and that may be intended to influence political, military, or economic conditions abroad while concealing U.S. sponsorship of another country prior to commencement of the principal operation. As noted in a 1990 SSCI report,

> The Committee would regard as "other-than-routine" support (requiring a finding and reporting to the committee) such activities as clandestinely recruiting and/or training of foreign nationals with access to the target country actively to participate in and support a U.S. military contingency operation; clandestine efforts to influence foreign nationals of the target country concerned to take certain actions in the event a U.S. military contingency operation is executed; clandestine efforts to influence and effect public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions in the event a U.S. military contingency operation is executed.
>
> In other words, the Committee believes that when support to a possible military contingency operation involves other than unilateral efforts by U.S. agencies in support of such operation, to include covert U.S. attempts to recruit, influence, or train foreign nationals, either within or outside the target country, to provide witting support to such operation, should it occur, such support is not "routine." *In such circumstances, the risks to the United States and the U.S. element involved have, by definition, grown to a point where a substantial policy issue is posed, and because such actions begin to constitute efforts in and of themselves to covertly influence events overseas* (as well as provide support to military operations).[25] [emphasis added]

Congress's discussion of *other-than-routine* support in open forums is limited to general discussion of covert action and routine support in the conference reports accompanying the Intelligence Authorization Act for 1991 (P.L. 102-88). It is not defined in statute and is not a term in DOD's lexicon. DOD categorizes these kinds of operations as *operational preparation of the environment* (OPE), a type of traditional military activity. This difference of perspective

[23] See the interview of former Deputy CIA Director, Michael Morell and former Commander of United States Special Operations Command, Admiral William McRaven, "The Road to Abbottabad: Ten Years Later," The Hayden Center, George Mason University, September 11, 2020, at https://www.youtube.com/watch?v=d7LbMfyZOZg. Morell described the raid as a covert action executed under a military chain of command.

[24] See CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary. See also Joint Pub 3-12, *Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, June 8, 2018), pp. X, GL-5, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[25] See U.S. Congress, Senate Select Committee on Intelligence, Authorizing Appropriations for Fiscal Year 1991 for the Intelligence Activities of the U.S. Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System, and for other Purposes, conference report to accompany S. 2834, 101st Cong., 2nd sess., July 10, 1990, S.Rept. 101-358, p. 55.

underscores the inherent tension between Title 10 and Title 50 authorities, insofar as the standards and processes for congressional notification of covert action—to include those Congress would categorize as other-than-routine support— differ from those for traditional military activities, including OPE. For an overview of congressional notification requirements for these activities, see CRS Report R45191, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements in Brief*, by Michael E. DeVine.

Clandestine Operations

Clandestine operations are *not* defined by statute. DOD defines a *clandestine operation as* "an operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment."[26] Clandestine operations are often thought of as relatively passive intelligence collection and information gathering operations. Unlike covert action, clandestine operations do not require a presidential finding, but they may require notification of Congress.

This definition differentiates *clandestine* from *covert*, using *clandestine* to signify the tactical concealment of the activity. By comparison, covert activities can be characterized as the strategic concealment of United States sponsorship of activities that aim to effect change in the political, economic, military, or diplomatic behavior of an overseas target. Because clandestine operations necessarily involve sensitive sources and methods of military operations or intelligence collection, their compromise, through unauthorized disclosure, potentially poses a risk to the lives of the personnel involved and may gravely damage U.S. national security.

Examples of clandestine activities include intelligence recruitment of, or collection by, a foreign intelligence asset; clandestine military operations in cyberspace; and military sensitive site exploitation of, or surveillance of, a facility in a denied or hostile area. Clandestine activities can be further categorized as *traditional military activities* or *routine* or *other-than-routine* support to traditional military activities, OPE, and *sensitive military operations*, all of which are discussed in more detail below. Clandestine activities can also be conducted in cyberspace in situations where both the activity and U.S. sponsorship are secret and unacknowledged.[27]

Traditional Military Activities and Routine Support to Traditional Military Activities

Since 9/11, as military and intelligence activities have become increasingly integrated, Congress has taken renewed interest in the two military exceptions to the statutory definition of covert action: *traditional military activities* and *routine support* to traditional military activities. Although the terms are not defined in statute, Congress's intent regarding *traditional military activities* and *routine support* to traditional military activities is relevant to understanding the range of military activities that involve less stringent notification requirements than those for covert action. These terms, which were first cited as exceptions to covert action in P.L. 102-88, the Intelligence Authorization Act for FY1991, may include activities that are difficult to distinguish from covert action or clandestine intelligence activities, which the military conducts under its Title 10 authorities.[28] In a joint explanatory statement attached to the conference report

[26] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms,* November 2021, p. 35, at https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.

[27] See CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary.

[28] 50 U.S.C. §3093(e).

to P.L. 102-88, the conference committee provided an extended discussion of its intent as to the meaning of *traditional military activities*:

> It is the intent of the conferees that 'traditional military activities' include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly. In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and control of a military commander should not be considered as "traditional military activities."[29]

In the SSCI conference report (S. Rept. 101-358) to the FY1991 Intelligence Authorization Act, the committee provided an expanded definition of the idea of *routine support* for congressional purposes:

> The Committee would regard as "routine support" such measures as providing false documentation, foreign currency, special communications equipment, maps, photographs, etc., to persons to be involved in a military operation that is to be publicly acknowledged. The Committee would also regard as "routine" support other unilateral actions that might be undertaken by elements of the U.S. Government within the target country itself, such as the caching of communications equipment or weapons, the leasing or purchase from unwitting sources of residential or commercial property to support an aspect of the operation, or the procurement and storage of vehicles and other equipment from unwitting sources to be used in such operations, if the operation as a whole is to be publicly acknowledged.[30]

Operational Preparation of the Environment

Operational Preparation of the Environment (OPE) is a DOD term for a category of traditional military activities conducted in anticipation of, in preparation for, and to facilitate follow-on military operations. It is a term DOD frequently uses, though its definition does not exist in statute. The DOD defines OPE as the "conduct of activities in likely or potential operational areas to set conditions for mission execution," with operational environment defined as "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[31] Examples of OPE could include close-in reconnaissance of a target, infrastructure development in a targeted area, or the reception, staging, onward movement and integration of forces in an anticipated area of operations.

Many in Congress have expressed concern that the military overuses OPE to describe a range of military activities, such as clandestine military intelligence collection, which do not clearly fall

[29] See U.S. Congress, House of Representatives Permanent Select Committee on Intelligence, *Intelligence Authorization Act, Fiscal Year 1991*, conference report to accompany H.R. 1455, 102nd Cong., 1st sess., July 25, 1991, H.Rept. 102-166, p. 29-30.

[30] See U.S. Congress, Senate Select Committee on Intelligence, Authorizing Appropriations for Fiscal Year 1991 for the Intelligence Activities of the U.S. Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System, and for other Purposes, conference report to accompany S. 2834, 101st Cong., 2nd sess., July 10, 1990, S.Rept. 101-358, pp. 54-55.

[31] See Joint Staff, "DOD Dictionary of Military and Associated Terms," November 2021, pp. 160, 161, at https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf.

within the oversight jurisdiction of either the congressional intelligence or congressional defense committees, and therefore, might escape Congress's notice altogether. In the "Areas of Special Interest" segment of the House Permanent Select Committee on Intelligence (HPSCI) report (H.Rept. 111-186) to its version of the Intelligence Authorization Act for FY2010 (H.R. 2701), the committee indicated that

> In categorizing its clandestine activities, DOD frequently labels them as "Operational Preparation of the Environment" (OPE) to distinguish particular operations as traditional military activities and not as intelligence functions. The Committee observes, though, that overuse of this term has made the distinction all but meaningless. The determination as to whether an operation will be categorized as an intelligence activity is made on a case-by-case basis; there are no clear guidelines or principles for making consistent determinations .... Clandestine military intelligence-gathering operations, even those legitimately recognized as OPE, carry the same diplomatic and national security risks as traditional intelligence-gathering activities. While the purpose of many such operations is to gather intelligence, DOD has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist. Consequently, these activities often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction.[32]

Eight years later, the HPSCI reiterated this sentiment. In a section titled "Jurisdictional Statement on Defense Intelligence" under the "Committee Priorities" segment of its report (H.Rept. 114-573) accompanying the Intelligence Authorization Act of 2017 (H.R. 5077), the HPSCI stated that it is

> ...concerned that many intelligence and intelligence-related activities continue to be characterized as 'battlespace awareness,' 'situational awareness,' and – especially – 'operational preparation of the environment' .... The continued failure to subject OPE and other activities to Committee scrutiny precludes the Committee from fully executing its statutorily mandated oversight role on behalf of the House and the American people, including by specifically authorizing intelligence and intelligence-related activities as required by Section 504(e) of the National Security Act of 1947 (50 U.S.C. §3094(e)). Therefore, the Committee directs [DOD] to ensure that the Committee receives proper insight and access to information regarding all intelligence and intelligence-related activities of [DOD], including those presently funded outside the MIP [Military Intelligence Program]. The Committee further encourages [DOD], in meeting this direction, to err on the side of inclusivity and not to withhold information based on arbitrary or overly technical distinctions such as funding source, characterization of the activities in question, or the fact that the activities in question may have a nexus to ongoing or anticipated military operations.[33]

Sensitive Military Operations

Sensitive military operations are defined in statute as (1) lethal operations or capture operations conducted by the U.S. Armed Forces outside a declared theater of active armed conflict, or conducted by a foreign partner in coordination with the U.S. Armed Forces that target a specific individual or individuals; (2) operations conducted by the U.S. Armed Forces outside a declared

[32] See U.S. Congress, House of Representatives Permanent Select Committee on Intelligence, "Intelligence Authorization Act for Fiscal Year 2010," report together with minority and additional views to accompany H.R. 2701, 111th Cong., 1st sess., June 26, 2009, H.Rept. 111-186, pp. 48-49.

[33] U.S. Congress, House of Representatives Permanent Select Committee on Intelligence, "Intelligence Authorization Act for Fiscal Year 2017," report together with minority views to accompany H.R. 5077, 114th Cong., 2nd sess., May 18, 2016, H.Rept. 114-573, pp. 9-10.

theater of active armed conflict in self-defense or in defense of foreign partners, including during a cooperative operation; or (3) an operation conducted by the U.S. Armed Forces to free an individual from the control of hostile foreign forces.[34] This statutory definition allows Congress to provide oversight of the sort of military operations that have significant bearing on U.S. foreign and defense policy but are not clearly defined elsewhere by statutory oversight provisions.

Sensitive military operations, which can be clandestine, became a common feature of the post-9/11 counterterrorism (CT) landscape involving U.S. military intervention in countries such as Yemen, Pakistan, or Somalia that were outside areas of active hostilities. Examples of these operations include a lethal CT drone operation, or military train, advise, and assist missions where U.S. forces supporting the security forces of a foreign partner nation may have to act in self-defense.

Clandestine Military Activities or Operations in Cyberspace

Section 1632 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) amended Section 394 of Title 10 of the *U.S. Code* by providing the statutory authority for DOD to conduct clandestine military activities or operations in cyberspace as a type of traditional military activity.[35] Clandestine military activities or operations in cyberspace include activities "short of hostilities ... or 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."[36] The Act defined clandestine military activity or operation in cyberspace as,

> a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary [of Defense] 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 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 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.[37]

Some of the congressional intent of this language was to provide DOD greater latitude to conduct operations in cyberspace under the military's Title 10 authorities without the greater oversight restrictions of covert action. The law's conference report explained the reasoning for classifying

---

[34] 10 U.S.C. §130f(d).

[35] Section 1632(3)(b)-(c) of P.L. 115-232:

> (b) Affirmation of Authority.--Congress affirms that the activities or operations referred to in subsection (a), when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (P.L. 93-148; 50 U.S.C. 1541 et seq.)) or 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.
>
> (c) Clandestine Activities or Operations.--A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

[36] Ibid.

[37] Ibid. Some internal numbering omitted.

these types of cyber operations as traditional military activities by noting the difficulties DOD previously has encountered in obtaining approval for cyberspace operations.

> One of the challenges routinely confronted by the Department is the perceived ambiguity as to whether clandestine military activities and operations, even those short of cyber attacks, qualify as traditional military activities as distinct from covert actions requiring a Presidential Finding. As a result, with respect to actions that produce effects on information systems outside of areas of active hostilities, the Department of Defense has been limited to proposing actions that could be conducted overtly on attributable infrastructure without deniability—an operational space that is far too narrow to defend national interests. The conferees see no logical, legal, or practical reason for allowing extensive clandestine traditional military activities in all other operational domains (air, sea, ground, and space) but not in cyberspace. It is unfortunate that the executive branch has squandered years in interagency deliberations that failed to recognize this basic fact and that this legislative action has proven necessary.[38]

Sensitive Military Cyber Operations

Sensitive military cyber operations are a subcategory of sensitive military operations. Depending upon the specific operation, they could be either conducted as a type of traditional military activity or—if accompanied by a presidential finding and conducted under Title 50 authority—as a covert action.[39] Congress defines sensitive military cyber operations under Title 10 as operations carried out by the Armed Forces of the United States that are intended to cause cyber effects against a foreign terrorist organization or country, including its armed forces and proxy forces, with which the United States is not engaged in hostilities, or with respect to which the involvement of the United States in hostilities has not been acknowledged publicly, which involve a medium to high degree of impact on the intended objective.[40] Sensitive military cyber operations have two subcategories, neither of which is defined in statute. The first, offensive cyberspace operations, is defined by DOD as "missions intended to project power in and through cyberspace."[41] The second, defensive cyberspace operations, is defined by DOD 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."[42]

---

[38] See U.S. Congress, House of Representatives Committee on Armed Services, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, P.L. 115-232, conference report to accompany H.R. 5515, 115th Cong., 2nd sess., July 25, 2018, H.Rept. 115-874.

[39] 10 U.S.C. §395(d)(2). "The notification requirement [for the Secretary of Defense to notify the congressional defense committees in writing within 48 hours of a sensitive military cyber operation] does not apply ... to a covert action." [some internal numbering omitted]

[40] 10 U.S.C. §395(c)(1)(A)-(B). Prior to reclassification and renumbering of the *U.S. Code*, the statute governing sensitive military cyber operations had been 10 U.S.C. §130(j).

[41] Offensive cyberspace operations are defined in Joint Pub 3-12, *Cyberspace Operations*, p. GL-5. See also note to §111 of Title 10 U.S.C., P.L. 112-81, div. A, title IV, §954, 125 Stat. 1551: "Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. §1541 et seq.)."

[42] For the DOD definition of offensive cyberspace operations, see Joint Publication 3-12, *Cyberspace Operations*, June 8, 2018, p. GL-5, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. Currently, statute does not define or describe offensive or defensive cyberspace operations. JP 3-12 p. GL-4 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."

Potential Considerations for Congress

- The characterization of intelligence and military activities determines, in part, committee jurisdiction over these matters. What measures exist that enable the congressional defense and intelligence committees to share notification information for clandestine operations conducted under Title 10 or Title 50 authority? How much and to what extent should Congress exert its power to provide specific direction to DOD for how certain activities should be shared with the congressional oversight committees?
- Should Congress establish with DOD a common view of "other-than-routine" support to traditional military activities, which the SSCI mentioned in its 1991 conference report (conference report to accompany S. 2834, 101st Cong., 2nd sess., July 10, 1990, S.Rept. 101-358, p. 55)?
- What are the potential disadvantages of not requiring a presidential finding for clandestine military cyber activities in cyberspace? In what respects do the objectives of clandestine military cyber activities resemble those of covert action?

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

Acknowledgments

Heidi Peters provided support to this report.

Disclaimer