(Illustration generated by DALL-E 3)

Practice Notes

Vigilance in Practice

The Role of Judge Advocates in Counterintelligence Investigations

By Major Michelle K. Lukomski

Counterintelligence is, in effect, chasing ghosts.[1]

Imagine the following: in a barracks room on Fort Campbell, Kentucky, Sergeant (SGT) Shady, a young U.S. Army military intelligence Soldier, uses an encrypted messenger app to communicate with a foreign national in Hong Kong. He has been talking to the individual for a few weeks, and a standard practice has developed: SGT Shady sends the foreign national information about the U.S. military, including classified information, in exchange for money. The foreign national, aware of SGT Shady's access to U.S. intelligence, provides collection priorities regarding the type of information he is interested in. Despite knowing that his actions are unlawful, SGT Shady shares information regarding the operability of sensitive U.S. military systems and capabilities, including documents and manuals related to field artillery equipment, aircraft, and intercontinental ballistic missiles.

This fictional scenario is not far from recent reality; the above facts are based on the real-world actions and eventual prosecution of SGT Korbein Schultz. Beginning in June 2022, and continuing for months after, Schultz willingly provided sensitive and classified

material to a foreign national in exchange for money.[2] The investigation of SGT Schultz was conducted jointly by the Federal Bureau of Investigation (FBI) and the U.S. Army Counterintelligence Command (ACIC).[3] Schultz was charged with violations of the Espionage Act, the Arms Export Control Act, and the International Traffic in Arms Regulations.[4] He pled guilty to all charged offenses on 13 August 2024.[5] In April 2025, he was sentenced to eighty-four months in prison.[6]

Public fascination with stories of espionage is evidenced by the volume of movies, television shows, and books on the subject.[7] While real-world examples of espionage usually do not involve Tom Cruise-worthy stunts, the threat to national security is no less damaging. National security crimes within the military are investigated by counterintelligence (CI) agents trained and authorized to investigate such offenses. CI agents across all military departments are trained to "detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize espionage, intelligence collection, sabotage, sedition, subversion, assassination, and terrorist activities . . . directed against U.S. national security interests or [Department of War (DoW)] and its personnel, information, materiel, facilities, and activities."[8]

CI investigations are conducted under both intelligence and criminal investigation authorities. The role of a judge advocate (JA) is similar to that in any other criminal investigation—to advise on the lawfulness of the agents' actions to preserve the integrity of the investigation. However, there are nuances to CI investigations, and JAs should be familiar with the unique legal challenges of a CI investigation.

Consider again SGT Shady: CI agents have reason to believe he printed classified documents and is storing them in a locker in his barracks room. They want to conduct a search to seize the evidence. The command is also aware that, since learning he is under investigation, SGT Shady has decided to flee. His commander is considering ordering him into pretrial confinement (PTC). The unit now has a need to access certain information about the ongoing CI investigation to meet the legal standard for PTC.[9] And because of the classified nature of the materials involved, much of the CI investigative details and documents are classified and highly compartmentalized.

As these additional hypothetical details suggest, while some aspects of a CI investigation mirror those of any other criminal investigation, there are unique challenges when national security crimes are involved. JAs must understand the legal obstacles CI agents will encounter as they address the emerging needs of their mission, and how to accurately advise.

This article serves as a resource to JAs charged with advising on these complex investigations. It explores the organizational structure and authorities of CI entities within the DoW, comparing how CI investigations are executed between the various Services. Understanding the similarities and differences of the various Service programs is critical to working alongside sister Services. It then discusses the role of the JA in the CI investigation process and provides recommendations for navigating search authorizations, PTC, and working with classified information. It also highlights new legislation impacting CI agents' authority, which will likely affect the role of Article II courts and judges in CI investigations.[10] Finally, it explores whether national security crimes should continue to be prosecuted by the Department of Justice (DoJ) rather than the DoW via courts-martial.

Counterintelligence Investigations Throughout the DoW

CI is "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities."[11] Put simply, CI is intended to thwart spying and other disruptive activity by the enemy. CI investigations are conducted across all military Services, but with some variation in process and structure depending on the Service. This section will focus on the CI structure and investigative authorities of the Army, Air Force, and Navy/Marine Corps.

Authorities Generally

As in all military operations, authority to conduct CI investigations begins with the U.S. Constitution. The President's Commander-in-Chief and foreign affairs powers under Article II, Section 2 are commonly understood to include an inherent authority to direct intelligence operations.[12] Pursuant to his constitutional authority, President Ronald Reagan issued Executive Order (EO) 12,333 in 1981.[13] EO 12,333 constitutes the foundational authority in intelligence activities and intelligence oversight, balancing national security interests with the privacy rights of U.S. persons.[14]

EO 12,333 designates the FBI as the lead agency for CI within the United States.[15] Authority to conduct CI activities is also granted to the DoW and intelligence and CI elements of the Army, Navy, Air Force, and Marine Corps.[16] Specifically, EO 12,333 directs the Secretary of War to "protect the security of [DoW] installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar association with the [DoW] as are necessary."[17]

Those agencies with authority to conduct intelligence activities, including CI, are authorized to "collect, retain, or disseminate information concerning United States persons," subject to procedures established by the responsible agency.[18] Importantly, CI investigations are generally conducted under these intelligence authorities.[19] However, there are circumstances, such as with SGT Schultz, where the investigation, or at least a part of it, is conducted under law enforcement authorities.[20] The distinction in authorities lies in the purpose of the investigation: where there is an intent to collect and preserve evidence that will eventually be used in a criminal prosecution, law enforcement authorities are required.[21]

CI investigators are required to coordinate with the FBI on CI investigations.[22] Coordination includes initial notification to the FBI of "any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power."[23] After the initial report, where a determination is made that the investigation will be jointly conducted by the CI entity

and the FBI, there is extensive coordination and communication between the agencies.[24]

CI Structure Across the DoW

Although there is significant overlap in the missions and authorities of the military departments' respective CI elements, the structure of the CI elements varies across Services.

ACIC

ACIC is a functional command within the U.S. Army Intelligence and Security Command (INSCOM) with the sole CI mission within the Army.[25] INSCOM is commanded by a two-star general and serviced by an office of the staff judge advocate at Fort Belvoir.[26] As a subordinate unit commanded by a one-star general, ACIC also has dedicated attorneys and paralegals assigned to advise and assist them in their mission.[27] ACIC is the Army entity charged with all CI activities to "detect, identify, neutralize, and exploit foreign entities, international terrorists, insider threats, and other foreign adversaries."[28] CI investigations are a method by which ACIC achieves its mission.[29] While the Army CI mission has existed for some time, ACIC was only recently established, evolving in 2021 from the former 902nd Military Intelligence Group and the INSCOM G2X Counterintelligence and Human Intelligence Division.[30]

ACIC agents are not considered law enforcement agents, but rather intelligence agents.[31] Notwithstanding, CI investigators may be responsible for processing forensic and physical evidence, interviewing witnesses, and preparing for criminal prosecution.[32] Despite the apparent law enforcement functions inherent in their mission, CI agents are limited by the authorities of intelligence agents, namely with regard to search authorizations, as discussed below.

The National Defense Authorization Act (NDAA) for Fiscal Year 2025 included new legislation that provides Army CI agents with some law enforcement functions.[33] The law allows civilian Army CI agents to serve warrants, execute searches, and make arrests.[34] The goal of the legislation is to align authorities for civilian Army CI agents with those of Civilian Defense Criminal Investigative Service (DCIS) and Civilian Army Criminal Investigation Command (CID) agents.[35] Of note, *uniformed* agents of DCIS, CID, and ACIC derive authority to serve warrants and make arrests under the Uniform Code of Military Justice (UCMJ). Irrespective of the new NDAA provision, the UCMJ currently allows for execution of searches, though military judges historically have not granted search authorizations for uniformed CI agents.[36]

Air Force Office of Special Investigations

The Air Force Office of Special Investigations (AFOSI) employs over 2,000 military and Civilian credentialed special agents, serving within seven field investigation regions aligned with Air Force major commands.[37] Unlike ACIC, AFOSI is a consolidated investigative entity responsible for criminal investigations, CI, and threat detection.[38] AFOSI "performs as a Federal law enforcement agency, a defense criminal investigative organization, a military criminal investigative organization, and a military department CI organization."[39]

AFOSI has relatively broad discretion to conduct investigative activities within the scope of its mission. For example, AFOSI agents are authorized to execute civilian search warrants for both UCMJ and non-UCMJ matters, and to arrest individuals not subject to the UCMJ with or without an arrest warrant in matters related to the AFOSI mission.[40] Overall, AFOSI has more latitude in its authorities and, therefore, capability as compared to ACIC.

Naval Criminal Investigation Service

The Naval Criminal Investigative Service (NCIS) is comprised of approximately 1,000 special agents and, similar to AFOSI, is tasked with the mission of both criminal and CI investigations within the Navy and Marine Corps.[41] Notably, NCIS is a Civilian-run agency, headed by a Civilian law enforcement professional who reports directly to the Secretary of the Navy.[42]

NCIS is the only Department of the Navy entity authorized to conduct CI investigations.[43] Similar to AFOSI, NCIS CI agents have broad discretion to conduct CI investigations under the supervision and authority of the NCIS director. As law enforcement officers, they have authority to conduct a wider range of investigative activities, whether in criminal or CI investigations.

Building the Case: Investigations to Trial

Just as criminal investigations collect and prepare evidence for criminal prosecutions, CI investigations may form the basis for the prosecution of national security crimes. Commonly, national security crimes, even when allegedly perpetrated by military members involving military information and intelligence, are prosecuted by the DoJ.[44] Practically, this may be for resourcing reasons, as the DoJ maintains entire teams of attorneys dedicated to national security prosecutions, and because the FBI, the investigative arm of the DoJ, may already be jointly conducting the investigation. Regardless of the prosecuting entity, ACIC investigations may rely on the advice and guidance of Army JAs to maintain the legal integrity of the case as the investigation progresses.

Applicable Criminal Offenses

The crimes being investigated will often inform a legal advisor's approach to the conduct of investigations. Thus, it is important for JAs to develop a basic knowledge of the national security crimes that may ultimately be charged. Categorizing national security crimes can be difficult, as national security law will often intersect with international criminal law, transnational criminal law, and domestic criminal law.[45] The overlap between these broad categories is based not only on the legal theory of criminalization, but also the "criminological profiles (i.e., their causes and methods of prevention), as well as the way in which law enforcement officials investigate and detect them."[46]

Notwithstanding the difficulties of creating a tidy list of national security crimes, there are some crimes in the U.S. Code and the UCMJ that are clearly designed to criminalize what might traditionally be considered national security offenses. The discussion below is not inclusive of all national security crimes, but rather those most prosecuted in the modern era.[47]

The U.S. Code

Treason and treason-related offenses (such as rebellion and insurrection), espionage, including the disclosure of classified information, and sabotage are all criminalized under Title 18 of the U.S. Code.[48] Espionage is commonly understood as the theft or

The ACIC patch. (Credit: Adam Lowe)

exploitation of national defense information, and it is generally the most identifiable of national security offenses.[49] The Espionage Act, codified in sections 791–799 of Title 18, criminalizes, among other things, gathering, transmitting, or losing defense information; gathering or delivering defense information to aid a foreign government; disclosure of classified information; and violating regulations of the National Aeronautics and Space Administration.[50]

Title 22 of the U.S. Code, which generally includes provisions related to foreign relations, also includes criminal penalties for violations of the Arms Export Control Act (AECA).[51] The AECA "confers authority on the President to control the import and export of defense goods and services," and promulgates regulations to protect defense technologies.[52] It further permits the President to establish a U.S. Munitions List (USML), which identifies and defines the defense articles subject to those regulations and controls.[53] This law tends to arise in national security investigations and prosecutions because "defense articles" include technical data for weapons systems, aircraft, missiles, and other implements of war designated on the USML.[54] Section 2778 goes on to establish criminal penalties for any willful violation of AECA or any rule or regulation thereunder.[55]

The UCMJ

In the UCMJ, relevant punitive articles include mutiny or sedition, spying, espionage, aiding the enemy, selling or otherwise disposing of military property, and unauthorized distribution of classified information or unauthorized access to a Government computer.[56] Although national security crimes are less commonly prosecuted at court-martial, these offenses have remained, and have been largely unchanged in structure and text, through multiple editions of the *Manual for Courts-Martial*.[57]

Espionage under the UCMJ is effectively the same offense as espionage under Title 18.[58] In Article 103a of the UCMJ, espionage requires proof that an accused, "with intent or reason to believe that [such matter would] . . . be used to the injury of the United States or to the advantage of a foreign nation, communicate[d], deliver[ed], or transmit[ted]" any material relating to the national defense to any foreign government or faction, party, "or military or naval force within a foreign country."[59] 18 U.S.C. § 793 contains almost the exact same statutory language, but provides a more comprehensive,

An ACIC Soldier analyzes a satellite image. (Source: ACIC)

though still non-exhaustive, list of what may be considered material relating to the national defense.[60] Sections 793 and 794 of Title 18 also create two distinct crimes: one for gathering, transmitting, or losing defense information, and one for actually delivering the information to a foreign government.[61]

National security offenses in the UCMJ are rarely seen in Army courts-martial.[62] However, it is foreseeable that other military-specific offenses will become relevant during a CI investigation or national security prosecution. For example, desertion or absence without leave, failure to obey orders or regulations, false official statement, conduct unbecoming an officer, and general Article 134 offenses may all arise as collateral misconduct.[63]

The Road to Trial

Search Authorizations

Most JAs will be familiar with search authorizations in the context of criminal investigations. In general, where there is an expectation of privacy, unconsented searches of on-post locations will require authorization based on a finding of probable cause.[64] In criminal investigations, authorizations may come from a military magistrate or a military judge.[65] Searches pursuant to a search authorization may then be executed by "any commissioned officer, warrant officer, petty officer, noncommissioned officer, and, when in the execution of guard or police duties, any criminal investigator, member of the Air Force security forces, military police, . . . or person designated by proper authority to perform guard or police duties."[66]

Military Rule of Evidence (MRE) 315(f)(2) states that the probable cause determination must find that "there is a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched."[67] By the terms of the MRE, there is no restriction on the use of search authorizations by CI agents; there is no explicit language limiting search authorizations only to criminal investigations conducted by agents of CID, AFOSI, NCIS, military police investigators, or other military law enforcement agency. However, in practice, military judges and military magistrates do not issue search authorizations in CI investigations. The primary obstacle to CI search authorizations is the classification of CI agents as intelligence agents rather than law enforcement agents.[68] Because CI agents begin their investigation for a CI purpose, and thus under intelligence authorities, there is a hesitancy to recognize that a CI agent may perform some law enforcement functions, including requesting and executing a search authorization.[69]

However, the new authorities in the 2025 NDAA explicitly permit law enforcement activities, including searches, which allow military judges to grant search authorizations in the same way they are granted to law enforcement agents.[70] Indeed, the legislation's goal was to put ACIC agents on level footing with CID agents for purposes of search authorizations and other law enforcement processes.[71] Thus, the new legislation should allow ACIC agents to leverage their law enforcement authorities as needed to request and execute search authorizations.[72]

Consider again SGT Shady. ACIC agents have reason to believe that he is storing classified material in his barracks locker until he can share it with his contact in Hong Kong. The barracks room would ordinarily be an area that a commander, military magistrate, or military judge would be able to grant authority to search. Importantly, the search would be for non-intelligence purposes—the goal is to secure evidence for prosecution. Thus, if supported by a properly sworn affidavit from a trained agent that provides sufficient evidence to establish probable cause, under the 2025 NDAA, a military judge could issue the search authorization to a Civilian CI agent.[73]

Pretrial Confinement (PTC)

There is no presumption of PTC in the military; an accused will only be ordered into PTC upon a showing of probable cause that an offense triable by court-martial has been committed, the accused committed it, and confinement is required by the circumstances.[74] Confinement may be required where it is foreseeable that the accused will not appear at trial or other proceeding, or will engage in serious criminal misconduct, and less severe forms of restraint are inadequate.[75]

Within the context of CI investigations, the requirements for PTC may be met by the facts associated with the national security crime(s) being investigated. However, whether PTC is appropriate may arise because of collateral misconduct. Suppose SGT Shady tells his battle buddy that he will take his chances on the run and go absent without leave (AWOL). He even tells his battle buddy that he has a bag packed and he plans to leave his cell phone behind so he cannot be tracked. Upon learning this information, the

The staircase over the INSCOM headquarters lobby displays the command's watch word: "Vigilance Always." (Source: INSCOM)

commander asks his servicing JA whether he can order the Soldier into PTC.

The PTC analysis may not deviate at all from what JAs are accustomed to: SGT Shady has certainly expressed a plan to go AWOL, and it is foreseeable that the Soldier will not appear at trial. There is also likely enough evidence to find probable cause that he committed an offense under the UCMJ, for example, espionage. Thus, the commander can order SGT Shady into PTC. Notably, because FBI and DoJ involvement in CI cases is common, a PTC decision should be discussed and coordinated with all interested parties.[76]

For example, in cases where the investigation is conducted jointly with the FBI and the DoJ has already expressed an intention to prosecute, there may be interest in applying restrictions or conditions on the Soldier that are similar to Federal bail standards rather than PTC.[77] This may gain efficiency in the eventual prosecution in Federal court—a prosecutor is saved from explaining a military justice process that a Federal judge may be unfamiliar with. Similarly, using lawful orders to restrict allows for some early advocacy because the written order can elucidate the underlying criminal offense and rely on the U.S. Code sections that will ultimately appear on the indictment rather than the UCMJ.[78]

JAs should maintain a role of bridging the communication gap between CI investigators and commanders to ensure that sufficient information is available to support a legally defensible determination. JAs should view their role as one of dual purpose: enabling commanders to make legally permissible decisions while also protecting the legal integrity of the ongoing CI investigation.

Classified Information Sharing

Some initial obstacles for CI investigations may be related to information sharing, as many CI investigations will involve classified information. Much has been written on the issue of information sharing.[79] Truly understanding information sharing issues and solutions is a necessary part of a JA's role in advising CI investigations and commanders. When classified information is included in any investigation, whether criminal or CI, spillage can affect the eventual availability of evidence for prosecution.[80]

The mechanism for sharing information, including information that a command would need to take UCMJ or other administrative action, is known as a letterhead

memorandum (LHM).[81] The LHM is used "to provide information about CI investigations to other Government agencies or organizations with a vested interest in the information or those that have preliminary jurisdiction and responsibility for responding to the incident."[82] Practically, the LHM will include administrative data and a summary of information obtained by ACIC agents, and it is recommended that LHMs be presented in-person to allow for further communication between the agents and the receiving unit or agency.[83] LHMs used by ACIC are generally identical to other Army memoranda, while other agencies, like the FBI, will use their own agency format.[84]

Returning once more to the investigation into SGT Shady, it is not difficult to see where information sharing issues would arise. Where the relevant offenses involve unauthorized access to and use of classified material under the Espionage Act, the investigative materials will necessarily include classified information. When the command contemplated PTC to prevent SGT Shady from going AWOL, the classified information may or may not be severable from the investigative details needed for a commander to make their determination. In either case, the LHM is a tailorable tool to share information that will promote efficiency in the overlapping processes of CI investigations and pretrial activities.

Whose Crime Is It Anyway?

Until very recently, the lack of law enforcement authorities for ACIC agents has contributed to a standard practice, at least with Army CI cases, of referring national security prosecutions of military members to the DoJ. Because of the limited law enforcement authorities, DoJ involvement is often required in the early phases of an investigation. Thus, referring the prosecution to the DoJ follows logically where the FBI and Federal judges have been involved in the case from the outset—and have ample resources—even though the military would have concurrent jurisdiction of national security cases involving Service members.

Concurrent jurisdiction between the DoJ and DoW is not a new phenomenon; indeed, a memorandum of understanding (MoU) between the two agencies regarding concurrent jurisdiction for investigations and prosecutions has existed since 1984.[85] The MoU recognizes the need for mutually reinforcing policies and procedures between the two agencies and explicitly states that "it is neither feasible nor desirable to establish inflexible rules regarding the responsibilities of the [DoW] and the [DoJ] as to each matter over which they may have concurrent interest."[86] Thus, although the MoU generally discusses certain crimes that the DoJ or DoW will have primary responsibility for, they are not strict mandates.

Notably, the MoU identifies "frauds against the [DoW] and theft and embezzlement of Government property" as crimes under the primary investigative authority of the DoW.[87] The DoW is required to confer with the DoJ and FBI on matters which, "if developed by investigation, would warrant Federal prosecution," but the DoJ is not specifically required to prosecute such cases.[88] SGT Shady's disclosure of classified materials to a foreign national could be considered fraud against the DoW or theft of Government property.[89] Therefore, after conferring with the DoJ and FBI, SGT Shady could be prosecuted by court-martial under the UCMJ.

Courts-martial for UCMJ national security offenses are a realistic possibility. The military would have personal jurisdiction over uniformed personnel accused of national security offenses.[90] A variety of national security offenses in the UCMJ closely mirror those in the U.S. Code, which can be brought to bear on a Service member. Some courtrooms throughout the Army are equipped to handle classified materials at court-martial, though more robust facilities would likely be required should these prosecutions become more frequent.[91] Perhaps the most important factor in the feasibility of retaining national security prosecutions is whether our military justice practitioners remain ready to execute these complex prosecutions if called upon to do so.[92]

With the enactment of legislation providing CI agents broader law enforcement authorities to execute searches and arrests, the military justice system is poised to take a more active role in pretrial procedures, namely, searches. With the potential increased involvement of military judges and JAs early on, justice may be more efficiently served by prosecution through courts-martial. Should there be such a shift, JAs will need to become comfortable with a more specific practice within military justice. National security prosecutions will almost certainly include classified materials. Therefore, while prosecutorial strategy may be similar to that of other criminal prosecutions, the technical presentation of evidence will be more nuanced.[93] By prioritizing the continued education and training of attorneys for national security prosecutions, the Judge Advocate General's (JAG) Corps can expand its impact and value, providing another level of efficiency and accountability in criminal procedure.

Conclusion

With the expansion of CI investigative authorities, practitioners within the military justice system will have the opportunity to broaden their practice. With dedicated training and resources, the JAG Corps can be prepared to prosecute national security crimes under the UCMJ. However, JAs must be prepared to advise CI investigations regardless of the eventual prosecuting agency. If CI investigations are, as Asha Rangappa said, like "chasing ghosts,"[94] CI agents will need to leverage all the tools and abilities available to them to achieve their mission; they will need competent and involved JAs to guide them in that pursuit. Cognizance of the unique nature of CI investigations is crucial for a JA to provide candid counsel for commanders and CI agents to enable the CI mission of a more secure force. **TAL**

MAJ Lukomski is an LL.M. candidate at Columbia Law School in New York.

Notes

1. A quote from former FBI agent and Yale lecturer Asha Rangappa. Linda McKendrick, *What Is Counterintelligence Law and Why It Matters More than Ever in 2025*, Law. Monthly (Apr. 7, 2025), https://www.lawyer-monthly.com/2025/04/counterintelligence-law-2025 [https://perma.cc/V3QE-DUV4].

2. Indictment ¶¶ 18–19, United States v. Schultz, No. 3-24-00056 (M.D. Tenn. Mar. 6, 2024) [hereinafter Schultz Indictment].

3. *U.S. Army Intelligence Analyst Pleads Guilty to Charges of Conspiracy to Obtain and Disclose National*

Defense Information, Export Control Violations and Bribery, Off. of Pub. Affs., U.S. Dep't of Just. (Aug. 23, 2024) [hereinafter *Schultz Press Release*], https://www.justice.gov/opa/pr/us-army-intelligence-analyst-pleads-guilty-charges-conspiracy-obtain-and-disclose-national [https://perma.cc/NP9H-L9WY].

4. *See* Schultz Indictment, *supra* note 2; 18 U.S.C. § 93(g); 22 U.S.C. § 2778.

5. *Schultz Press Release*, *supra* note 3.

6. *Former U.S. Army Intelligence Analyst Sentenced for Selling Sensitive Military Information to Individual Tied to Chinese Government*, Off. of Pub. Affs., U.S. Dep't of Just. (Apr. 23, 2025), https://www.justice.gov/opa/pr/former-us-army-intelligence-analyst-sentenced-selling-sensitive-military-information [https://perma.cc/J62P-R2FV].

7. *See, e.g.*, Dr. No (Eon Productions 1962); No Time to Die (Eon Productions 2021); Hunt for Red October (Paramount Pictures 1990); The Americans (FX 2013–2018); The Blacklist (NBC 2013–2023); Bridge of Spies (MGM 2015); The Good Shepherd (Universal Pictures 2006); Mission Impossible (Paramount Pictures 1996–2025).

8. U.S. Dep't of Def., Dir. 5240.02, Counterintelligence para. 3 (17 Mar. 2015) (C1, 16 May 2018) [hereinafter DoDD 5240.02].

9. PTC is discussed more fully *infra* Section titled "Pretrial Confinement." To order a Soldier into PTC, a commander must determine that (1) an offense triable by court-martial has been committed; (2) the person being confined committed it; (3) confinement is necessary because it is foreseeable that the confinee will not appear at trial, pretrial hearing, or preliminary hearing, or the confinee will engage in serious criminal misconduct; and (4) less severe forms of restraint are inadequate. Manual for Courts-Martial, United States, R.C.M. 305(i)(2)(B) (2024) [hereinafter MCM 2024].

10. Article II courts and judges refer to courts and judges within the executive branch, thus organized and administered under Article II of the U.S. Constitution. They include administrative courts and military courts, and are created under authority delegated to the President by Congress. *See Article II Tribunal (Article II Court or Article Two Court)*, The Wolters Kluwer Bouvier Law Dictionary (Desk ed. 2012).

11. DoDD 5240.02, *supra* note 8, pt. II, at 12–13 (defining CI).

12. U.S. Const. art. II, § 2; *see also* Major Alexander Morningstar, *Distinguishing Between Operational and Intelligence Activities: A Legal Framework*, Army Law., no. 4, 2022, at 63, 65 (citing Joshua Kuyers, *"Operational Preparation of the Environment": "Intelligence Activity" or "Covert Action" by Any Other Name*?, 4 Nat'l Sec. L. Brief 21, 37 (2013)).

13. Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *amended by* Exec. Order Nos. 13,284, 13,355, and 13,470 (July 30, 2008) [hereinafter Exec. Order No. 12,333].

14. Morningstar, *supra* note 12, at 64.

15. Exec. Order 12,333, *supra* note 13, paras. 1.7(g), 1.13. The Central Intelligence Agency is responsible for CI outside the United States; the Defense Intelligence Agency also has authority within the United States "to support national and departmental missions." *Id*. para. 1.7(a)(2), (b)(1).

16. *Id.* para. 1.7(f).

17. *Id.* para. 1.10(h).

18. *Id.* para. 2.3. Collection of information is further guided and restricted by Department of Defense Manual 5240.01. U.S. Dep't of Def., Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities (8 Aug. 2016) [hereinafter DoDM 5240.01].

19. *See* Exec. Order 12,333, *supra* note 13, paras. 1.7, 1.13.

20. *See* Schultz Indictment, *supra* note 2; *Schultz Press Release*, *supra* note 3.

21. Generally, unconsented physical searches for intelligence in the United States are not authorized unless conducted by the FBI in accordance with applicable laws and procedures, which often include searches governed by the Foreign Intelligence Surveillance Act (FISA). 50 U.S.C. §§ 1801–29, 1841–46, 1861–62, 1871; *see also* Telephone Interviews with Carl Johnson, Senior Nat'l Sec. L. Att'y, Off. of the Judge Advoc. Gen. (Nov. 1, 2024; Dec. 18, 2024) [hereinafter Interviews with Mr. Johnson]. There are circumstances where an investigation might begin under intelligence authorities, and might include information obtained through a FISA warrant, but then subsequently the investigation becomes, at least partially, criminal in nature. Interviews with Mr. Johnson, *supra*. The information collected under intelligence authorities may then be used as a basis for additional investigation under law enforcement authorities. *Id.* For example, information collected through a FISA warrant may subsequently be used in an affidavit for a search authorization as part of the criminal investigation. *Id.*

22. Exec. Order 12,333, *supra* note 13, para. 1.14(a). Practically, notifications to the FBI may be done formally using a letterhead memorandum, as discussed more fully *infra* Section titled "Classified Information Sharing," or more informally through communications between CI agents and FBI agents in the applicable field office. Telephone Interviews with Caroline Pascal, Senior Civilian Legal Advisor, Army Counterintelligence Command (Sep. 27, 2024; Dec. 18, 2024) [hereinafter Interviews with Mrs. Pascal].

23. 50 U.S.C. § 3381(e)(1)(A).

24. *Id.*

25. U.S. Army Intel. & Sec. Command, https://www.usainscom.army.mil/MSCs [https://perma.cc/7QX3-V6SG] (last visited Dec. 29, 2025).

26. *Commanding General*, U.S. Army Intel. & Sec. Command, https://www.usainscom.army.mil/Organization/Commanding-General [https://perma.cc/8JXH-BS3F] (last visited Dec. 29, 2025) (identifying Major General Timothy J. Brown as the current INSCOM commanding general); The Judge Advoc. Gen.'s Corps, U.S. Army, JAGC Personnel Directory 270 (1 Oct. 2024) [hereinafter JAGC Directory] (identifying the INSCOM Office of the Staff Judge Advocate personnel).

27. U.S. Army Counterintelligence Command, https://www.usainscom.army.mil/MSCs/ACIC [https://perma.cc/2HR5-PABS] (last visited Dec. 29, 2025); JAGC Directory, *supra* note 26, at 273.

28. *Major Subordinate Commands*, U.S. Army Intel. & Sec. Command, https://www.usainscom.army.mil/MSCs [https://perma.cc/TB5N-YY7B] (last visited Dec. 29, 2025).

29. U.S. Army Counterintelligence Command, *supra* note 27.

30. *Id.*

31. U.S. Off. of Pers. Mgmt., Handbook of Occupational Groups and Families 27, 109 (Dec. 2018). ACIC agents are coded as 0132 positions, which are intelligence activities positions, not 1811, which are criminal investigation positions.

32. *See* U.S. Army Counterintelligence Command, *supra* note 27.

33. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, sec. 1613, 138 Stat. 1773, 2173 (2024); *see also* Interviews with Mr. Johnson, *supra* note 21.

34. Sec. 1613, 138 Stat. at 2173.

35. 10 U.S.C. §§ 1585a, 7377, respectively; *see also* Interviews with Mr. Johnson, *supra* note 21.

36. MCM 2024, *supra* note 9, M.R.E. 315(e). As discussed *infra* Section titled "The Road to Trial," military judges hesitate to acknowledge that CI agents can switch between their intelligence mission and law enforcement functions. Thus, although MRE 315(e) would allow uniformed CI agents to conduct searches, military judges have treated requests for search authorizations from CI agents as for intelligence purposes. Once implemented, the legislation should provide the statutory support for a culture shift in which military judges are comfortable considering search authorizations for CI agents, both uniformed and Civilian.

37. *Lines of Effort*, U.S. Air Force Office of Special Investigations, https://www.osi.af.mil/About/Fact-Sheets/Display/Article/349945/office-of-special-investigations [https://perma.cc/ER4Y-JSDM] (last visited Dec. 29, 2025).

38. *See id.*

39. U.S. Dep't of Air Force, Pol'y Dir. 71-1, Criminal Investigations and Counterintelligence para. 3.2 (1 July 2019).

40. *Id.* para. 3.2.5.

41. *See About NCIS*, U.S. Naval Crim. Investigation Serv., https://www.ncis.navy.mil/About-NCIS [https://perma.cc/4MHZ-5Q59] (last visited Dec. 29, 2025).

42. *Id.*

43. U.S. Dep't of Navy, Sec'y of Navy Instr. 3850.2E, Department of the Navy Counterintelligence, para. 5.g (3 Jan. 2017).

44. *See generally National Security Division*, U.S. Dep't of Justice, https://www.justice.gov/nsd [https://perma.cc/W2YV-CSPV] (last visited Dec. 29, 2025) (stating the mission of the Department of Justice National Security Division); *see also* Schultz Indictment, *supra* note 2; *U.S. Army Soldier Sentenced to 14 Years in Prison For Attempting to Assist ISIS to Conduct Deadly Ambush on U.S. Troops*, U.S. Dep't of Just. (Oct. 11, 2024), https://www.justice.gov/opa/pr/us-army-soldier-sentenced-14-years-prison-attempting-assist-isis-conduct-deadly-ambush-us [https://perma.cc/NAK3-LWDT].

45. *See* Erin Creegan, *National Security Crime*, 3 Harv. Nat'l Sec. J. 373, 374–75 (defining international criminal law as "violations of international law perpetrated by state actors," and transnational criminal law as "cooperation between states to tackle threats posed by more 'ordinary' criminal activities," including terrorism,

human trafficking, and organized crime, and national security law as addressing "threats against the security of a state and its people as such, whether they come from another state or a transnational or even domestic group").

46. *Id.* at 375.

47. *See Press Releases*, Off. of Pub. Affs., U.S. Dep't of Just., https://www.justice.gov/news/press-releases [https://perma.cc/2RRU-7AVB] (last visited Dec. 29, 2025) (displaying most recent press releases from the DoJ, which routinely include information about national security prosecutions involving espionage, sabotage, and terrorism).

48. U.S. Const. art. III, § 3; 18 U.S.C. § 2381 *et seq.* (treason and treason-related offenses); 18 U.S.C. § 793 *et seq.* (espionage); 18 U.S.C. §§ 2152–56 (sabotage of defenses during a time of war); 18 U.S.C. §§ 1362–68 (malicious mischief related to communication lines, station or systems, buildings or property within special maritime and territorial jurisdiction, consumer products, energy facilities, satellite systems, and law enforcement animals). Terrorism crimes may also be considered within the broad category of national security crimes; however, the legal paradigm for criminal prosecutions in recent years is one focused on criminalizing the terrorist for being a terrorist, rather than the terrorist act. *See* Creegan, *supra* note 45, at 403–04 (discussing the predominant use by the DoJ of post-9/11 terrorism statutes that criminalize material support to terrorists or designated terrorist organizations and receipt of military-type training from a foreign terrorist organization). As such, the criminalized acts are generally subsumed by the other common national security offenses, though prosecuted under terrorism laws due to the status of the offender. *Id.* at 404.

49. *See* 18 U.S.C. § 793; Creegan, *supra* note 45, at 386.

50. 18 U.S.C. §§ 791–99.

51. 22 U.S.C. §§ 2751–2799aa-2.

52. Creegan, *supra* note 45, at 397.

53. 22 U.S.C. § 2778(a).

54. *Id.* § 2778(b)(2); *see also* Schultz Indictment, *supra* note 2, ¶ 13 (explaining that SGT Schultz's disclosure of technical data to a another person without the required license to do so constitutes a violation of the Arms Export Control Act).

55. 22 U.S.C. § 2778(c).

56. *See* UCMJ arts. 94 (2011), 103 (2016), 103a (2016), 103b (2016), 108 (2011), 123 (2016).

57. *See id.* Changes to arts. 103, 103a, 103b, and 123 in 2016 were solely renumbering; substantively, they have remained unchanged.

58. *See* UCMJ art. 103a (2016).

59. *Id.*

60. *See* 18 U.S.C. § 793(a).

61. *See* 18 U.S.C. §§ 793, 794. In the UCMJ, the former would likely be prosecuted as attempted espionage. *See* UCMJ art. 103a (2016).

62. *See* Off. of the Judge Advoc. Gen., U.S. Navy, U.S. Navy Report on Military Justice for Fiscal Year 2023 para. 4.h. (2023) [hereinafter U.S. Navy Report on MJ for FY23] (describing only three national security courts-martial prosecuted in fiscal year 2023 by the U.S. Navy).

63. UCMJ arts. 85 (2019), 86 (1956), 92 (1950), 107 (2016), 133 (2021), 134 (2016).

64. MCM 2024, *supra* note 9, M.R.E. 315. This discussion will focus on on-post locations; off-post locations would almost always require a warrant from an Article III judge and would require coordination with the FBI for execution. There are some searches that do not require prior authorizations or a determination of probable cause. *See id.* M.R.E. 314 (consent, border, Government property). Commanders may authorize searches of Government property, which generally includes on-post locations where there is no expectation of privacy. *See id.* M.R.E. 314(d). For example, an Army commander may authorize CID to search the supply cages within a unit area as part of an investigation into suspected theft of Government property.

65. *Id.* M.R.E. 315(b). While search authorizations are issued by appropriate military authority, "search warrants" are issued by "competent civilian authority" under R.C.M. 703A and similarly provides authority for a probable cause search.

66. *Id.* M.R.E. 315(e)(1).

67. *Id.* M.R.E. 315(f)(2).

68. Interviews with Mr. Johnson, *supra* note 21.

69. *Id.*

70. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, sec. 1613, 138 Stat. 1773, 2173 (2024).

71. Interviews with Mr. Johnson, *supra* note 21.

72. Importantly, CI agents will need to ensure that they are wearing the correct "hat" at any given time during an investigation; searches for intelligence purposes will still be governed by intelligence authorities, specifically Procedure 7 of DoDM 5240.01. DoDM 5240.01, *supra* note 18, at 35.

73. It would be preferable for the CI agent(s) that are intimately involved in the case to be swearing out and submitting the affidavit in support of the request. Historically, CI agents might involve CID as a partner in the investigation and allow their agents sufficient access to evidence and information such that a CID agent can swear to the affidavit and request the search authorization. While it achieves the desired end state, it is less efficient and introduces unnecessary complexity that may detract from the presentation of evidence at trial. *See* Interviews with Mr. Johnson, *supra* note 21; Interviews with Mrs. Pascal, *supra* note 22.

74. MCM 2024, *supra* note 9, R.C.M. 305(d).

75. *Id.* R.C.M. 305(i)(2)(B).

76. Interviews with Mrs. Pascal, *supra* note 22.

77. *Id*. This would be accomplished through a lawful order by the commander that adopts specific language regarding bail restrictions to ensure consistency with Federal standards.

78. *Id*.

79. *See, e.g.*, Ashley Deeks, *Secrecy Surrogates*, 106 Va. L. Rev. 1395 (2020); Valerie J. Pelton, *The Enemy Among Us: The Insider Threat*, 82 J. Air L. & Com. 519 (2017); Ann Koppuzha, *Secrets and Security: Overclassification and Civil Liberty in Administrative National Security Decisions*, 80 Alb. L. Rev. 501 (2016); Oona A. Hathaway et al., *Congressional Oversight of Modern Warfare: History, Pathologies, and Proposals for Reform*, 63 Wm. & Mary L. Rev. 137 (2021); Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C. L. Rev. 585 (2016).

80. Major Michael Petrusic, *Navigating Government Information Protections and Privileges: Using Protected Government Information in Courts-Martial*, Army Law., July 2017, at 20.

81. *See* U.S. Dep't of Army, Pam. 381-20, Counterintelligence Investigative Procedures para. 2-45(g)(3) (15 Apr. 2020).

82. *Id.* para. 2-45(g)(1).

83. *See id.* Depending on the investigation and the information conveyed, LHMs may be classified or unclassified.

84. Interviews with Mrs. Pascal, *supra* note 22; Army Regulation 25-50 provides the formatting requirements for Army memoranda. *See* U.S. Dep't of Army, Regul. 25-50, Preparing and Managing Correspondence paras. 2–4 (10 Oct. 2020).

85. *See* U.S. Dep't of Def., Dir. 5525.07, Implementation of the Memorandum of Understanding between the Dep'ts of Just. and Def. Relating to the Investigation and Prosecution of Certain Crimes fig. 1 (5 Mar. 2020) (depicting the verbatim text of the original 1984 MoU).

86. *Id.* fig. 1, para. B.

87. *Id.* fig. 1, para. C(1)(b).

88. *Id.*

89. The MoU does not identify specific provisions of the U.S. Code as fraud or theft crimes. *See id.* SGT Schultz was charged with violations of the Arms Export Control Act, which could arguably be considered a fraud against the DoW and theft of Government property since the factual basis for the charge was the unlawful disclosure of defense articles to a foreign national. *See* Schultz Indictment, *supra* note 2, ¶¶ 20–29.

90. *See* MCM 2024, *supra* note 9, R.C.M. 202; UCMJ art. 2 (2023).

91. Interviews with Mr. Johnson, *supra* note 21.

92. *See* U.S. Navy Report on MJ for FY23, *supra* note 62, para. 4.h(3), at 10 (describing the U.S. Army Advocacy Center Classified Litigation Course designed to provide students with training in national security prosecutions).

93. MRE 505 will feature prominently in national security prosecutions. Generally, MRE 505 prohibits military judges from releasing classified information to any person not authorized to receive it. *See* MCM 2024, *supra* note 9, M.R.E. 505. It further provides procedures for the proper handling of classified information when it is relevant to a court-martial. *See id.* The interplay of classified material with privileges and discovery in general can lead to complex pretrial litigation. *See id.*

94. *See supra* note 1 and accompanying text.