CHAPTER 14

AUTHORITIES FOR HOMELAND DEFENSE (HD) OPERATIONS

An addendum to the

DOMESTIC OPERATIONAL LAW HANDBOOK

2024

FOR LEGAL PERSONNEL

CENTER FOR LAW AND MILITARY OPERATIONS

November 2024

Given the Army's refocus on large-scale combat operations, near peer competitors, and Homeland Defense generally, CLAMO asked Mr. Robert Gonzales, National Security Law Attorney at U.S. Army North, to put together an additional chapter for the DOPLAW Handbook. Mr. Gonzales is one of the Army's foremost subject matter experts in Domestic Operational Law. In years past, the focus of the Handbook has been solely Defense Support to Civil Authorities, with no information about the other major category of domestic operations. The addition of this chapter highlights the importance of Homeland Defense for the military legal practitioner. Special thanks to Mr. Gonzales as the primary author of this chapter, with significant contributions regarding unmanned systems and information activities from Mr. Ljubisa Pejic.

CONTRIBUTING AUTHORS AND EDITORS FOR THIS ADDENDUM

Mr. Robert Gonzales
Mr. Ljubisa Pejic
MAJ Alexander Morningstar
CPT Kristin Capes
CPT Michael Caswell

Continued thanks to all contributors to this and prior editions of the Domestic Operational Law Handbook.

Center for Law and Military Operations (CLAMO)
The Judge Advocate General's Legal Center and School, U.S. Army
Charlottesville, VA 22903-1781

CHAPTER 14

AUTHORITIES FOR HOMELAND DEFENSE (HD) OPERATIONS

KEY REFERENCES:

- U.S. CONST. art. I, § 8 (Declare War Clause).
- U.S. CONST. art. II, § 2 (Commander in Chief Clause).
- U.S. CONST. art. IV, § 4 (Guarantee Protection Clause).
- 6 U.S.C. § 466, Sense of Congress reaffirming the continued importance and applicability of the Posse Comitatus Act (2023).
- 10 U.S.C. § 113, Secretary of Defense (2023).
- 10 U.S.C. § 123, Authority to suspend officer personnel laws during war or national emergency (2023).
- 10 U.S.C. §130i, Protection of certain facilities and assets from unmanned aircraft (2023).
- 10 U.S.C. § 138, Assistant Secretaries of Defense (2023).
- 10 U.S.C. § 162, Combatant Commands: assigned forces (2023).
- 10 U.S.C. § 164, Commanders of combatant commands: assignment; powers and duties (2023).
- 10 U.S.C. §§ 251-254, Insurrection Act (2023).
- 10 U.S.C. § 801(16), Definition of National Security.
- 10 U.S.C. § 2644, Control of transport systems in time of war (2023).
- 10 U.S.C. § 2663, Land acquisition authorities (2023).
- 10 U.S.C. § 2674, Operation and control of Pentagon Reservation and defense facilities in National Capitol Region (2023).
- 10 U.S.C. § 4882, Industrial mobilization: orders; priorities; possession of manufacturing plants; violations (2023).
- 10 U.S.C. §§ 12301-12304, Reserve Component (2023).
- 10 U.S.C. § 12310, Reserves: for organizing, administering, etc., reserve components (2023).
- 18 U.S.C. § 32, Destruction of aircraft or aircraft facilities (2023).
- 18 U.S.C. § 1385, Posse Comitatus Act (2023).
- 18 U.S.C. §§ 2510-2523, Wire and Electronic Communications Interception and Interception of Oral Communications Act (2023).
- 18 U.S.C. §§ 3121-3127, Pen Registers and Trap and Trace Devices Act (2023).
- 18 U.S.C. § 1030, Fraud and related activity in connection with computers (2023).
- 18 U.S.C. § 1362, Communication lines, stations or systems (2023).
- 18 U.S.C. § 1367, Interference with the operation of a satellite (2023).
- 18 U.S.C. § 1801, Video voyeurism, (2023).
- 32 U.S.C. § 901-908, National Guard Homeland Defense Activities (2023).
- 40 U.S.C. § 71, Physical development of National Capitol (2023).

- 40 U.S.C. § 1310, Sale of war supplies, land, and buildings (2023).
- 40 U.S.C. § 8702, Physical development of National Capitol Region (2023).
- 42 U.S.C. § 1313, Assistance for citizens returned from foreign countries (2023).
- 46 U.S.C. § 7005, Regulation of anchorage and movement of vessels during national emergency (2023).
- 47 U.S.C. § 333, Willful or malicious interference (2023).
- 47 U.S.C. §§ 501-511, Penal Provisions; Forfeiture (2023).
- 47 U.S.C. § 606, War powers of the President (2023).
- 49 U.S.C. § 40103, Sovereignty and use of airspace (2023).
- 49 U.S.C. § 46307, Violation of national defense airspace (2023).
- 49 U.S.C. § 46502, Aircraft piracy, (2023)
- 50 U.S.C. § 98, Strategic and Critical Materials Stock Piling Act (2023).
- 50 U.S.C. § 1541, War Powers Resolution (2023).
- 50 U.S.C. § 1621, *et seq.*, National Emergencies Act (2023).
- 50 U.S.C. § 1631, Declaration of national emergency by Executive order; authority; publication in Federal Register; transmittal to Congress (2023).
- 50 U.S.C. § 2313, Nuclear, chemical, and biological emergency response (2023).
- 50 U.S.C. § 2314, Pub. L. 104-201, Under Secretary of Defense for Policy (2023).
- 50 U.S.C. §§ 3001 – 3243, National Security Act of 1947 (2023).
- Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707 (1988).
- Taiwan Relations Act, Pub. L. No. 96-8, 93 Stat.14.
- John Warner National Defense Authorization Act Fiscal Year 2007, Pub. L. No. 109-364, 120 Stat. 2085 (2006).
- National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, sec. 1435 (2013).
- National Defense Authorization Act for Fiscal Year 2024, Pul. L. No. 118-31, sec. 1532 (2023).
- National Security Intelligence Reform Act, 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
- Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, 118 Stat.3688 (2004).
- 14 C.F.R. § 1.1, General definitions.
- 14 C.F.R. § 99.7, Special security instructions.
- 14 C.F.R. § 107, Small Unmanned Aircraft Systems.
- United States Intelligence Activities, Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).
- Ordering the Ready Reserve of the Armed Forces to Active Duty and Delegating Certain Authorities to the Secretary of Defense and the Secretary of Transportation, Exec. Order No. 13,223, 66 Fed. Reg. 48,201 (Sep. 14, 2001).
- Further Amendments to Executive Order 12333, United States Intelligence Activities, Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008).

- Ordering the Selected Reserve and Certain Individual Ready Reserve Members of the Armed Forces to Active Duty, Exec. Order No. 13,680, 79 Fed. Reg. 63,287 (Oct. 16, 2014).
- National Emergency Authority to Order the Selected Reserve and Certain Members of the Individual Ready Reserve of the Armed Forces to Active Duty, Exec. Order No. 13,912, 85 Fed. Reg. 18,407 (Mar. 27, 2020).
- Ordering the Selected Reserve of the Armed Forces to Active Duty, Exec. Order No. 13,919, 85 Fed. Reg. 26,591 (Apr. 30, 2020).
- Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade, Exec. Order No. 14059, 86 Fed. Reg. 71549 (Dec 15, 2021).
- Authority To Order the Ready Reserve of the Armed Forces to Active Duty to Address International Drug Trafficking, Exec. Order No. 14,097, 88 Fed. Reg. 26,471 (Apr. 27, 2023).
- Ordering the Selected Reserve and Certain Members of the Individual Ready Reserve of the Armed Forces to Active Duty, Exec. Order No. 14,102, 88 Fed. Reg. 45,807 (Jul. 13, 2023).
- Declaration of National Emergency by Reason of Certain Terrorist Attacks, Proclamation No. 7463, 66 Fed. Reg. 181 (Sep 14, 2001).
- Declaring a National Emergency Concerning the Southern Border of the United States, Proclamation No. 9844, 84 Fed. Reg. 4949 (Feb 15, 2019).
- Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak, Proclamation No. 9994, 85 Fed. Reg. 15337 (Mar 13, 2020).
- Continuation of the National Emergency with Respect to the Global Illicit Drug Trade, 87 Fed. Reg. 76549 (Dec 12, 2022).
- Continuation of the National Emergency with Respect to the Global Illicit Drug Trade, 88 Fed. Reg. 86809 (Dec 13, 2023).
- Presidential Policy Directive – 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013).
- North Atlantic Treaty, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
- Mutual Defense Treaty, U.S. – S. Kor., Oct. 1, 1953, 5 U.S.T. 2368.
- Mutual Defense Treaty, U.S. – Philippines, August 30, 1951.
- Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.
- DepSecDef Policy Memorandum 17-00X, Supplemental Guidance for Countering Unmanned Aircraft, July 5, 2017
- DoD Homeland Defense Policy Guidance, 12 December 2023 (SECRET).
- DoD/DHS Defense Infrastructure Base Plan, May 2010.
- Department of Defense Directive 2310.01E, DoD Detainee Program, March 15, 2022.
- Department of Defense Directive 2311.01, DoD Law of War Program, 2 July 2020.
- Department of Defense Directive 3020.40, Mission Assurance 12, 29 November 2016, Incorporating Change 1, 11 September 2018.

- Department of Defense Directive 3160.01, Homeland Defense Activities Conducted by the National Guard, 25 August 2008, Incorporating Change 2, 6 June 2017.
- Department of Defense Directive 5148.13, Intelligence Oversight, 26 April 2017.
- Department of Defense Directive 5240.01, DoD Intelligence Activities, 27 August 2007, Incorporating Change 3, 9 November 2020.
- Department of Defense Instruction 2000.12, DoD Antiterrorism (AT) Program, 1 March 2012, Incorporating Change 3, 8 May 2017.
- Department of Defense Instruction 3025.21, Defense Support of Civilian Law Enforcement Agencies, 27 February 2013, Incorporating Change 1, 8 February 2019.
- Department of Defense Instruction 3115.07, Signals Intelligence (SIGINT), 15 September 2008, Incorporating Change 2, 25 August 2020.
- Department of Defense Instruction 5505.17, Personally Identifiable Information and Law Enforcement Information Handling by DoD Law Enforcement Activities, August 22, 2023.
- Department of Defense Instruction 5400.11, DoD Privacy and Civil Liberties Programs, with Change 1, December 8, 2020.
- Department of Defense Instruction 8110.01, Mission Partner Environment Information Sharing Capability Implementation for the DoD, 30 June 2021.
- Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instr. 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, Encl. L, para. 1a (13 Jun. 2005) (SECRET).
- Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instr. 3125.01B, Defense Support of Civil Authorities (DSCA) for Domestic Consequence Management (CM) Operations in Response to a CBRNE Incident (19 August 2009).
- Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instr. 3320.01 Series, Joint Electromagnetic Spectrum Operations.
- Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Manual 3130.06C, Global Force Management Allocation Policies and Procedures, Enclosure C, 7 May 2021 (SECRET).
- Joint Staff Standing EXORD for Land Homeland Defense, 162252ZJAN15 (SECRET//REL TO FVEY).
- Joint Staff Domestic CBRN Response EXORD (CUI), 241452ZMAR16.
- Joint Staff message for Rules for the Use of Force (RUF) for QRF/RRF Ground Security Operations, 072310ZAUG03 (SECRET//REL TO USA AND CAN).
- Joint Publication 3-0, Joint Campaign and Operations, 18 June 2022.
- Joint Publication 3-01, Countering Air and Missile Threats, 6 April 2023.
- Joint Publication 3-27, Homeland Defense, 12 December 2023.
- Joint Publication 4-05, Joint Mobilization Planning, 2018.
- 2022 Unified Command Plan, 88 Fed. Reg. 26,219 at 13 – 14 (Apr. 25, 2023).
- Forces Command (FORSCOM) EXORD ISO Homeland Defense FY23, 281400ZJUL22 (SECRET).

- FORSCOM EXORD ISO CBRN CRE FY24, 191515ZMAY23.
- Army Regulation 381-10, The Conduct and Oversight of U.S. Army Intelligence Activities, 27 January 2023.
- Army Regulation 405-10, Acquisition of Real Property and Interests Therein, 1 August 1970.
- Field Manual 3-63, Detainee Operations, January 2020.
- Department of the Army, Office of The Judge Advocate General, DAJA-AL 2002/0238, Subject: G-1 Mobilization Round Table Discussion Issues, 18 March 2002
- Appendix 2 to Annex C to USARNORTH Supporting Plan to USNORTHCOM CONPLAN 3768-17, *Protection, Evacuation, Repatriation Operations in Response to Crises Abroad,* September 25, 2018.
- Final Report of the Special Committee on National Emergencies and Delegated Emergency Powers, U.S. Senate, S. Rep. No. 94-922 (1976).
- Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications, RL31133, Congressional Research Service (2014).
- Department of Justice Memorandum for the Honorable Robert E. Jordan III, General Counsel, Department of the Army, re: Authority to use troops to protect federal functions, including the safeguarding of foreign embassies in the United States, May 11, 1970.
- Defense Critical Infrastructure: Actions Needed to Improve the Consistency, Reliability, and Usefulness of DoD's Tier 1 Task Critical Asset List, GAO-09-740R, U.S. Government Accountability Office (2009).
- National Emergency Repatriation Framework, Department of Health and Human Services, Administration for Children & Families (2010).
- NCR-IADS Exhibit P-40, Budget Line-Item Justification, Battle Control System, February 2019.
- *Ex Parte Milligan*, 71 U.S. 2, 139 (1866).
- *United States v. Sweeny*, 157 U.S. 281, 284 (1895).
- John Cherry and Michael Rizzotti, *Understanding Self-Defense and the Law of Armed Conflict,* Articles of War, Lieber Institute, United States Military Academy, West Point, NY, March 9, 2021.
- Elbridge Colby, "*A Strategy of Denial for the Western Pacific,"* Proceedings, March 2023, Vol 149/3/1,441.
- Major Edward Faiello and Captain Brian McCracken, "Detainee Operations: Transition from Counterinsurgency to Large-Scale Combat Operations," *The National Security Law Quarterly,* Volume 23-4, pages 16-22, 27 November 2023
- SGT Brad Mincey, *263rd AAMDC validates, certifies training for NCR deployment*, U.S. ARMY (28 Jul 2016), https://www.army.mil/article/172376/263rd_aamdc_validates_certifies_training_for_ncr_deployment.
- Theodore Roosevelt, *An Autobiography* (New York: Macmillan, 1913), pp. 388-389.

- Martin Shapiro and Rocco J. Tresolini, *American Constitutional Law* (Fourth Edition), Chapter 6, War, Foreign Affairs, and the Presidency, pages 164-173.
- Albert L. Strum, "Emergencies and the Presidency," *Journal of Politics,* vol. 11, February 1949, pp. 125-126.
- William Howard Taft, *Our Chief Magistrate and His Powers* (New York: Columbia University Press, 1916), pp. 139-140.
- Norman M. Wade, HDS1 Smartbook, "Homeland Defense & DSCA," The Lightning Press, p. 1-2.
- Jessica Casserly, *Hanscom Looks to Modernize NCR Defense System*, Jessica Casserly, 66th Air Base Group Public Affairs, December 9, 2020.
- https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/
- https://www.defense.gov/News/Releases/Release/Article/3586406/united-states-japan-republic-of-korea-trilateral-ministerial-meeting-unilateral/Dec 19, 2023
- United States-Japan-Republic of Korea Trilateral Ministerial Meeting Joint Press Statement, Department of Defense, Jun 2, 2024.
- https://www.arnorth.army.mil/About/Mission/
- https://www.cbirf.marines.mil
- https://lieber.westpoint.edu/understanding-self-defense-law-armed-conflict/
- https://www.nato.int/cps/en/natohq/topics_110496.htm.
- https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/,
- https://www.senate.gov/about/powers-procedures/declarations-of-war.htm#:
- https://www.dhs.gov/publication/national-strategy-aviation-security
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/
- https://www.faa.gov/uas/getting_started/where_can_i_fly/airspace_101
- https://www.faa.gov/uas/resources/community_engagement/no_drone_zone
- https://www.hsdl.org/c/view?docid=472111

NOTE: Some of the footnotes are documents that have classified markings. However, all the information lifted from these documents into this chapter came from unclassified portions of these classified documents.

A. Introduction

The Constitution and Acts of Congress provide the framework for the President of the United States and/or Congress to authorize, initiate, and place the Nation in a Homeland Defense (HD) posture. HD is defined as the military protection of U.S. sovereignty and territory against external threats and aggression or, as directed by the President, other threats.[1] The homeland is the physical region that includes the

[1] JOINT CHIEFS OF STAFF, J. PUBL'N 3-27, HOMELAND DEFENSE, I-1 (12 DECEMBER 2023) [hereinafter JP 3-27].

continental United States (CONUS), Alaska, Hawaii, and territories in the Pacific (i.e., Guam, American Samoa, the Northern Mariana Islands), as well as territories in the Caribbean (i.e., the United States Virgin Islands, Puerto Rico, and the surrounding territorial waters and airspace).[2] Once the Nation is on an HD footing, the Department of Defense (DoD) will be the lead federal agency (LFA).[3] Then, every DoD person in the homeland will have the personal responsibility to support protecting the homeland. Each person will have a real and concrete role to play.[4] In this regard, it will be incumbent for every U.S. Army Judge Advocate (JA) stationed on the homeland to be knowledgeable about (1) the authorities the President may exercise, through the Secretary of Defense (SecDef) and (2) the legal issues and concerns commanders should take into consideration when planning for and executing military operations in a contested homeland environment. This chapter aims to provide an orientation and prepare those JAs who will be engaged in the National Defense Strategy's (NDS) number one priority: Homeland Defense.[5]

B. Major Strategic Competitors and U.S. Mutual Defense Agreements

Currently, the NDS identifies two major global threat competitors that the U.S. military competes against every day and who are primarily in two separate strategic regions: Russia in Eastern Europe and the People's Republic of China (PRC) in the Western Pacific.[6] The U.S. has military obligations and commitments in both regions, the fulfillment of which is intended to deter attacks by these two competitors against the homeland.

The most important defense agreement is the U.S.'s membership in the North Atlantic Treaty Organization (NATO). Founded on April 4, 1949, NATO's military purpose is to protect the territory and people of its European and North American member countries through the principle of collective defense against a possible Russian threat in Eastern Europe and other parts of the continent.[7] Article 5 provides if a NATO member is the victim of an armed attack, each and every other member of the alliance will consider this act of violence as an armed attack against all members who will each take the action it deems necessary to assist the member attacked.[8] For U.S. purposes, it is important to remember that Article 6 limits the geographical scope of the treaty. NATO covers the territory of any of the parties in Europe or North America, on the Algerian Departments of France, on the territory of Turkey or on the islands under the jurisdiction of any of the parties in the North Atlantic area north of the Tropic of Cancer.[9] Thus,

---

[2] *Id.*

[3] *Id.*

[4] HOMELAND DEFENSE POLICY GUIDANCE, pgs. 2 and 22, 12 December 2023 (SECRET).

[5] U.S. DEP'T OF DEFENSE, 2022 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA, p. 5 (2022).

[6] *Id.* at 2.

[7] *Collective Defence and Article 5*, NORTH ATLANTIC TREATY ORGANIZATION (Jul. 4, 2023, 11:47 AM), https://www.nato.int/cps/en/natohq/topics_110496.htm.

[8] North Atlantic Treaty, art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[9] *Id.* art. 6.

NATO does not include the State of Hawaii and the U.S. territories of Guam, the Virgin Islands, and Puerto Rico, which are all located south of the Tropic of Cancer.

The U.S. has several commitments in the Western Pacific, especially where the U.S. has forces stationed. A Mutual Defense Treaty between the U.S. and the Republic of South Korea (ROK) was signed on October 1, 1953, two months after the signing of the Korean Armistice Agreement, which brought a halt to the fighting in the Korean War. The agreement commits the two countries to provide mutual aid if either faces external armed attack and allows the U.S. to station military forces in South Korea in consultation with the South Korean government.[10]

The Treaty of Mutual Cooperation and Security between Japan and the U.S. is a treaty that permits the presence of U.S. military bases on Japanese soil and commits the two nations to defend each other if one or the other is attacked. The current treaty, which took effect on June 23, 1960, revised and replaced an earlier version of the treaty, which was signed in 1951.[11]

On December 19, 2023, the U.S. enhanced its commitment with ROK and Japan by announcing the activation of real-time Democratic People's Republic of Korea (DPRK) missile warning data sharing mechanism and an agreement for a multi-year trilateral exercise plan. The three countries established this mechanism to improve their ability to respond to regional challenges and ensure the peace and stability on the Korean Peninsula and the Northeast Asia region. The exercise plan will regularize trilateral exercises and execute them more systematically and efficiently in the future.[12]

Additionally, the SecDef and the Defense Ministers of the ROK and Japan convened a Trilateral Ministerial Meeting on June 2, 2024, in Singapore. The SecDef reaffirmed the U.S.'s ironclad commitment to the defense of Japan and the ROK, emphasizing its commitment is backed by the full range of U.S. capabilities, including conventional and nuclear.[13]

The U.S. has no formal defense treaty with Taiwan. Instead, the U.S. foreign policy towards Taiwan is stated in the Taiwan Relations Act of 1979.[14] It is the policy of the U.S. to (1) expect that the future of Taiwan will be determined by peaceful means, (2) consider any effort to determine the future of Taiwan by other than peaceful means a threat to the peace and security of the Western Pacific region, (3) provide Taiwan with arms of a defensive character, and (4) maintain the capacity to resist any resort to force or other forms of coercion that would jeopardize the security of the people on Taiwan.[15]

---

[10] Mutual Defense Treaty, U.S. – S. Kor., Oct. 1, 1953, 5 U.S.T. 2368.

[11] Treaty of Mutual Cooperation and Security, U.S. – Japan, Jan. 19, 1960, 11 U.S.T. 1632.

[12] DEPARTMENT OF DEFENSE, DEC 19, 2023, *UNITED STATES-JAPAN-REPUBLIC OF KOREA TRILATERAL MINISTERIAL*, [JOINT PRESS STATEMENT] https://www.defense.gov/News/Releases/Release/Article/3621235/united-states-japan-republic-of-korea-trilateral-ministerial-joint-press-statem/

[13] DEPARTMENT OF DEFENSE, JUN 2, 2024, *UNITED STATES-JAPAN-REPUBLIC OF KOREA TRILATERAL MINISTERIAL*, [JOINT PRESS STATEMENT] https://www.defense.gov/News/Releases/Release/Article/3793913/united-states-japan-republic-of-korea-trilateral-ministerial-meeting-tmm-joint/

[14] Taiwan Relations Act, Pub. L. No. 96-8, 93 Stat. 14 (codified as amended at 22 U.S.C. §§ 3301-16 (2023)).

[15] 22 U.S.C. § 3301(b) (2023).

Only 125 miles from Taiwan and the geographical link between Japan and Australia, the Philippines is the fourth Asian country to strengthen a deterrence relationship with the U.S. On May 3, 2023, the SecDef and the Philippine Secretary of the Department of National Defense established the Bilateral Defense Guidelines to modernize alliance cooperation in service of the U.S. and the Philippines' shared vision for a free and open Indo-Pacific region. The guidelines reaffirm that an armed attack in the Pacific, including anywhere in the South China Sea, on either of their public vessels, aircraft, or armed forces – which includes their Coast Guards – would invoke mutual defense commitments under Articles IV and V of the 1951 U.S.-Philippines Mutual Defense Treaty.[16]

The U.S.'s credibility in the Western Pacific is linked directly to Taiwan's defense against the PRC. If Beijing could take Taiwan, it would break out of the first island chain that currently constrains its military power projection. If the U.S. and its allies in the region can prevent the PRC from subordinating Taiwan, they can protect other U.S. allies in Asia, enabling the coalition to stand strong, checking Beijing's ambition to regional hegemony.[17]

C. Homeland Defense (HD) as a Subset of National Security

National Security includes both national defense and the foreign relations of the United States.[18] Stated another way, it is the safekeeping of the nation as a whole. Either way, understanding that the PRC and Russia represent direct threats to the national security of the United States, the President relies on the SecDef and two Combatant Commanders (CCDR) – United States Northern Command (USNORTHCOM) and United States Indo-Pacific Command (USINDOPACOM), for the national security of the homeland by both CCDRs performing HD in their respective area of responsibility (AOR).[19] For purposes of this chapter and to repeat, HD is defined as the military protection of U.S. sovereignty and territory against external threats and aggression or, as directed by the President, other threats.[20]

DoD protects the homeland through two distinct, but interrelated core missions: HD and Defense Support of Civil Authorities (DSCA). DoD may execute HD alone or with all

---

[16] U.S. DEP'T OF DEFENSE, FACT SHEET: U.S.-PHILIPPINES BILATERAL DEFENSE GUIDELINES (May 3, 2023).

[17] Elbridge Colby, "*A Strategy of Denial for the Western Pacific,"* Proceedings, March 2023, Vol 149/3/1,441.

[18] 10 U.S.C. § 801(16) (2023).

[19] 2022 UNIFIED COMMAND PLAN, 88 FED. REG. 26,219 AT 13 – 14 (APR. 25, 2023). THERE ARE CURRENTLY 11 UNIFIED COMBATANT COMMANDS, FOUR FUNCTIONAL AND SEVEN GEOGRAPHICAL. THE FOUR FUNCTIONAL COMBATANT COMMANDS OPERATE WORLD-WIDE ACROSS GEOGRAPHICAL BOUNDARIES AND PROVIDE UNIQUE CAPABILITIES TO THE GEOGRAPHIC COMBATANT COMMANDS AND THE ARMED SERVICES, WHILE THE GEOGRAPHICAL COMBATANT COMMANDS OPERATE IN CLEARLY DELINEATED AREAS OF RESPONSIBILITY AND HAVE A REGIONAL MILITARY FOCUS. THE FOUR FUNCTIONAL COMBATANT COMMANDS ARE SPECIAL OPERATIONS COMMAND (SOCOM), TRANSPORTATION COMMAND (TRANSCOM), STRATEGIC COMMAND (STRATCOM), AND CYBER COMMAND (CYBERCOM).

[20] JP 3-27, *supra* note 1, I-10 and GL-5.

sectors of U.S. society and government, including Federal, State, local, tribal, and territorial (SLTT) governments, and private sector partners that support DoD's efforts to defend the homeland.[21] DoD's role in the DSCA mission consists of DoD support to (1) U.S. civil authorities (Department of Homeland Security, Federal Emergency Management Agency (FEMA), and SLTT civil authorities) for presidential-declared major disasters or emergencies pursuant to the Robert T. Stafford Disaster Relief and Emergency Assistance Act, (2) civilian law enforcement agencies (DSCLEA), (3) the United States Secret Service (USSS) for National Special Security Events(NSSE), and (4) other domestic incidents. While these two missions are distinct, HD and DSCA operations may occur simultaneously and require extensive integration, coordination, and synchronization.[22] Undoubtedly, unique and complex legal issues will arise prior to and during the planning and conduct of land HD operations that will require the professional and competent advice from all JAs.[23]

Focusing solely on HD within the USNORTHCOM AOR, the combatant commander relies on U.S. Army North (ARNORTH), as its Theater Joint Force Land Component Command (JFLCC), to prepare for and protect the sovereignty and independence of the U.S. land domain. More specifically, ARNORTH is posed and prepared to (1) assume operational control of dedicated ground forces anywhere in the continental United States and Alaska to deter, detect, and defeat threats against the U.S. and the American people and (2) protect and defend DoD assets and capabilities to maintain its ability to actively project combat power around the globe.[24]

To this end, the following seventeen legal considerations for the planning and conducting of land HD missions within USNORTHCOM will hereafter be discussed in order: (1) President's Role in HD, (2) Congress' Role in HD, (3) Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs' Role in HD, (4) Initiation of HD, (5) Mobilization of Units and Members of the Reserve Component for HD, (6) Mission-Specific Rules for the Use of Force (RUF) for Land HD, (7) Levels of Detention Operations for Enemy Prisoners of War (EPW), (8) the Posse Comitatus Act (PCA) and HD, (9) Protection of Defense Critical Infrastructures (DCI) and Other Designated Properties, (10) Confiscation of Private Property for HD, (11) the Quick Response Force/ Rapid Response Forces (QRF/RRF) for HD, (12) Chemical, Biological, Radiological or Nuclear Response Force for HD, (13) National Capitol Region-Integrated Air Defense System (NCR-IADS), (14) Unmanned Aircraft Systems and Countermeasures during HD, (15) Intelligence and Information Gathering Activities during HD, (16) HD Activities by the National Guard, and (17) Repatriation of U.S. Citizens. This chapter will address HD in the air, maritime, cyber, and space domains only as it relates directly to land HD within the USNORTHCOM AOR.

---

[21] HOMELAND DEFENSE POLICY GUIDANCE, *supra* note 4, at 26

[22] HDS1 Smartbook, Homeland Defense & DSCA, Norman M. Wade, The Lightning Press, p. 1-2.

[23] JOINT STAFF STANDING EXORD FOR LAND HOMELAND DEFENSE, PARAGRAPH 5.L. (UNCLASSIFIED), 162252ZJAN15 (SECRET//REL TO FVEY) [HEREINAFTER JS HD EXORD].

[24] *Mission,* U.S. ARMY NORTH, https://www.arnorth.army.mil/About/Mission/ (last visited Nov. 8, 2023).

D. President's Role in HD

How the President views his role as Commander-in-Chief of the Armed Forces will determine how quickly, aggressively, and more importantly, legally, he will (1) direct the SecDef to deploy and employ military forces and (2) apply any of the vast number of emergency authorities at his disposal to defend the homeland against an external threat.

It was President Theodore Roosevelt's stewardship theory "that every executive officer in high position, was a steward of the people," and it was his sincere belief that for the President, "it was not only his right, but his duty to do anything that the needs of the Nation demanded, unless such action was expressly forbidden by the Constitution or by the laws."[25] Opposing this view of the presidency was Roosevelt's former Secretary of War, William Howard Taft, and his personal choice for and actual successor as President. Taft viewed the President's powers in more limited legal terms, writing, "that the President can exercise no power which cannot be fairly and reasonably traced to some specific grant of power or justly implied and included within such express grant as proper and necessary to its exercise." Under his constitutional theory, such a "specific grant must be either in the Constitution or in an act of Congress passed in pursuance thereof. There is," Taft concluded, "no undefined residuum of power which he can exercise because it seems to him to be in the public interest."[26] Between these two theories of the presidency are various gradations of legal opinions, resulting in as many conceptions of the office as there have been office holders. One presidential scholar and historian accurately summed up the situation in the following words: "In the final analysis, the power of a President is largely determined by the President himself."[27]

In the context of land HD, regardless of whatever philosophical perspective the President takes, he will rely on the DoD to protect the homeland against traditional external and internal threats or aggression and against asymmetric threats that are outside the scope of homeland security operations.[28] The homeland that must be defended is the physical region that includes the continental U.S. (CONUS), Alaska, Hawaii, and territories in the Pacific and in the Caribbean, including surrounding territorial waters and airspace.[29]

To buttress the President's ability to conduct HD and protect the Nation successfully, Congress has enacted approximately 470 contingency statutes conferring special emergency powers to the President and the executive branch.[30] At least one hundred and six (106) of these statutes apply to DoD. Most of the statutorily delegated emergency powers exist on a stand-by basis and are activated only after (1) the enactment of a declaration of war by Congress, (2) the existence of a state of war as

---

[25] THEODORE ROOSEVELT, AN AUTOBIOGRAPHY 388-9 (1913).

[26] WILLIAM HOWARD TAFT, OUR CHIEF MAGISTRATE AND HIS POWERS 139-40 (1916).

[27] Albert L. Strum, *Emergencies and the Presidency*, 11 JOURNAL OF POLITICS 121, 125-6 (1949).

[28] JP 3-27, *supra* note 1, I-1.

[29] *Id.*

[30] U.S. SENATE, FINAL REPORT OF THE SPECIAL COMMITTEE ON NATIONAL EMERGENCIES AND DELEGATED EMERGENCY POWERS, S. REP. NO. 94-922 at 5 (1976).

determined by the President, or (3) the promulgation of a National Emergency Declaration (NED) by either the President or Congress.[31]

The great majority of these emergency powers, including many of the most sweeping ones, can be activated only when the President issues a NED. An "authorization for the use of military force resolution," by itself and in contrast to a declaration of war or a NED, does not trigger any of these 470 standby authorities and powers.[32] Under these statutorily delegated emergency powers, the President may, for example, authorize taking possession and control of any system of transportation and communications;[33] seizing any factory equipped to manufacture arms, munitions, and war supplies;[34] the selling of war supplies and equipment to any foreign government engaged in war against a country with which the U.S. is at war;[35] and delegating to the Secretary of Homeland Security the authority to safeguard all vessels, harbors, ports, and waterfront facilities in the U.S. against destruction, loss, or injury.[36]

Within DoD, the President may mobilize members and units in the Reserve Component;[37] use, sell, or otherwise dispose of materials in the National Defense Stockpile;[38] defer any end-strength limitation for any military or civilian component of the DoD until six months after the war or national emergency terminates;[39] and acquire any interest in private land needed for national defense purposes immediately upon the filing of a Petition for Condemnation and an Order for Immediate Possession in Federal District Court.[40]

E. Congress' Role in HD

The Framers of the Constitution clearly intended the defense of the homeland to be a joint enterprise between the President and the Congress. Arguably, Congress has more responsibility than the President for HD, as evidenced by the Constitution giving it the power "To . . . provide for the common Defence . . .; To declare War . . .; To raise and support Armies . . .; To provide and maintain a Navy . . .; and to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions."[41]

---

[31] CONGRESSIONAL RESEARCH SERVICE, DECLARATIONS OF WAR AND AUTHORIZATIONS FOR THE USE OF MILITARY FORCE: HISTORICAL BACKGROUND AND LEGAL IMPLICATIONS, RL31133 at Summary (2014) (currently undergoing revision) [hereinafter CRS Report RL3113]. This is a very god source for a comprehensive list of the President's vast emergency powers.
[32] *Id.* at 43.
[33] 10 U.S.C. § 2644 (2013) and 47 U.S.C. § 606 (2023).
[34] 10 U.S.C. § 4882 (2023).
[35] 40 U.S.C. § 1310 (2023).
[36] 46 U.S.C. § 70051 (2023).
[37] 10 U.S.C. §§ 12301-12304 (2023).
[38] 50 U.S.C. § 98f(a)(2) (2023).
[39] 10 U.S.C. 123a (2023). statutes
[40] 10 U.S.C. 2663(b) (2023).
[41] U.S. CONST. art I, § 8.

Concerning the respective HD powers exercised by the Congress and by the President, Chief Justice of the Supreme Court, Samuel Chase, in 1866 explained the extent of Congress' authority in his concurring opinion in Ex Parte Milligan:

"Congress has the power not only to raise and support and govern armies, but to declare war. It has therefore the power to provide by law for carrying on war. This power necessarily extends to all legislation essential to the prosecution of war with vigor and success, except such as interferes with the command of the forces and the conduct of campaigns. That power and duty belong to the President as commander-in-chief."[42]

Later, Supreme Court Justice Henry Brown wrote that "the object of the [commander-in-chief clause of the Constitution] is evidently to vest in the President the supreme command over all the military forces -- such supreme and undivided command as would be necessary to the prosecution of a successful war."[43]

In the aftermath of World War II, Congress asserted its congressional powers by enacting the National Security Act of 1947 to realign and reorganize the U.S. Armed Forces into three military departments with the intent to provide a comprehensive program for the future security of the United States[44] An amendment in 1949 provided that the military departments would compose a Department of Defense and be separately administered under the direction of a Secretary of Defense.[45] Another amendment in 1958 inserted provisions relating to the establishment of Unified and Specific Combatant Commands with a clear and "direct line of command" from the SecDef to such commands.[46]

In passing the Goldwater–Nichols Department of Defense Reorganization Act of 1986, Congress again affirmed its statutory authority to make sweeping changes to DoD by reworking the "direct line of command."[47] It increased the powers of the Chairman of the Joint Chiefs of Staff.[48] It also streamlined the military chain of command to run from the President through the SecDef directly to the Combatant Commanders (CCDRs, all four-star generals or admirals), bypassing the Service secretaries and chiefs of staff.[49] The Service Secretaries and Chiefs of Staff were assigned to an advisory role to the President, the National Security Council, the SecDef, and the Congress, and given the responsibility for training and equipping units and personnel for future duty under one of the combatant commands.[50]

---

[42] *Ex Parte Milligan*, 71 U.S. 2, 139 (1866).
[43] *United States v. Sweeny*, 157 U.S. 281, 284 (1895).
[44] National Security Act of 1947, Pub. L. No. 80-253, 69 Stat. 495 (codified as amended at 50 U.S.C. §§ 3001 – 3243 (2023)).
[45] National Security Act Amendments of 1949, Pub. L. No. 81-216, 63 Stat. 578.
[46] Department of Defense Reorganization Act of 1958, Pub. L. No. 85-599, 72 Stat. 514.
[47] The Goldwater-Nichols Department of Defense Reorganization Act, Pub. L. No. 99-433, 100 Stat. 992.
[48] 10 U.S.C. § 151 (2023); 10 U.S.C. § 153 (2023).
[49] 10 U.S.C. § 162(b) (2023); 10 U.S.C. § 164(b) (2023).
[50] 10 U.S.C. § 151 (2023); 10 U.S.C. § 3013 (2023); 10 U.S.C. § 3033 (2023); 10 U.S.C. § 5013 (2023); 10 U.S.C. § 5033 (2023); 10 U.S.C. § 8013 (2023); 10 U.S.C. § 8033 (2023).

F. Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs' Role in HD

Congress continued to strengthen the civilian authority and organization of the DoD by establishing the position of Assistant Secretary of Defense for Homeland Defense (ASD(HD)) in the National Defense Authorization Act (NDAA) for Fiscal Year 2003.[51] The title was changed to Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs in 2009 and then to Assistant Secretary of Defense for Homeland Defense and Global Security in 2014. In 2022 the title was again changed to Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs (ASD(HD&HA). Through all these changes, one responsibility remained constant – HD. The mission of the Office of the ASD(HD&HA) is to provide policy and planning oversight for HD and mission assurance, DSCA, Arctic and Global Resilience, and Western Hemisphere Affairs matters as well as advance and represent priority issues with U.S. interagency partners, U.S. Congress, Allies and partners, U.S. SLTT governments, and private section organizations.[52]

In September 2003, the ASD(HD) was assigned the additional responsibility for Defense Critical Infrastructure (DCI) Protection and the lead for DoD's role as Sector Specific Agency for the Defense Industrial Base, as specified in the National Strategy to Secure Cyberspace (February 2003), the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February 2003), and Homeland Security Presidential Directive - 7 Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003) (See paragraph L below). Additionally, on January 6, 2006, the President signed into law the NDAA for Fiscal Year 2006.[53] Section 1031 provided that "[t]he Assistant Secretary of Defense for Homeland Defense is responsible for the coordination of DoD assistance to Federal, State, and local officials in responding to threats involving nuclear, radiological, biological, chemical weapons or high-yield explosives or related materials or technologies, including assistance in identifying, neutralizing, dismantling, and disposing of nuclear, radiological, biological, chemical weapons, and high-yield explosives and related materials and technologies (See paragraph O below)."[54]

Thus, the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs has the statutory responsibility for the overall supervision of the HD activities of

---

[51] Bob Stump National Defense Authorization Act for Fiscal Year 2003, Pub. L. No. 107-314, 116 Stat. 2620 (codified as amended at 10 U.S.C. § 138(b)(3) (2023)).

[52] *Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs*, U.S. SECRETARY OF DEFENSE FOR POLICY, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/ (last visited Nov. 7, 2023).

[53] *Assistant Secretary of Defense for Homeland Defense and Global Security Frequently Asked Questions*, U.S. SECRETARY OF DEFENSE FOR POLICY, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-and-Hemispheric-Affairs/Homeland-Defense-Integration-and-DSCA/faqs (last visited Nov. 7, 2023); National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163 (2006).

[54] National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163, 119 Stat. 3428 (codified as amended at 50 U.S.C. § 2313(a) (2023)).

the Department of Defense, including HD plans, the commitment of forces or other DoD resources, and the readiness posture of forces to conduct HD against any threat.[55]

G. Initiating HD

The Constitution of the United States is a document of enumerated and separated powers. With respect to the President, it states the President "shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual service of the United States."[56] The President also possesses the constitutional authority to protect every State when threatened by invasion.[57] Furthermore, he has statutory authority to declare a national emergency pursuant to Title 50 U.S.C. §§ 1621 and 1631. The powers relative to HD are not, however, confined to the Executive branch. Instead, the President shares HD authorities and responsibilities with the Legislative branch.

The Constitution vests in Congress the power "To declare War."[58] Pursuant to this power, Congress has enacted eleven declarations of war during the course of American history relating to five different wars, the most recent being those that were adopted during World War II.[59] Since World War II, the President and Congress have embraced the practice of Congress passing and the President signing into law a number of "authorizations for the use of military force resolution," such as the joint resolution enacted on September 18, 2001, authorizing the use of military force against terrorist [60] after President George W. Bush issued a National Emergency Declaration (NED) on 14 September 2001 for the attack in New York City and on the Pentagon on 9/11.[61]

H. Mobilization of Units and Members in the Reserve Component for HD?

When active-duty land forces are deployed overseas into the theater of hostilities, the homeland and its population and critical infrastructures may be very vulnerable to an attack. In order to defend the homeland, the President will call to active duty and mobilize units and members in the Reserve Component, which is composed of the Ready Reserve, Retired Reserve, and Standby Reserve, for defense of the homeland.

Title 10 U.S.C. §12301(a): "Full Mobilization" of the entire Reserve Component may be ordered by a Service Secretary IAW Title 10 U.S.C. § 12301(a), but only after Congress

---

[55] DEP'T OF DEFENSE, DIR. 5111.13, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY (ASD(HD&GS)) (23 Mar. 2018).
[56] U.S. CONST. art. II, § 2.
[57] U.S. CONST. art. IV, § 4.
[58] U.S. CONST. art. I, § 8.
[59] *About Declarations of War by Congress,* UNITED STATES SENATE, https://www.senate.gov/about/powers-procedures/declarations-of-war.htm#: (last visited Nov. 8, 2023).
[60] Authorization for Use of Military Force Against September 11 Terrorists, Pub. L. No. 107-40, 115 Stat. 224 (codified as 50 U.S.C. § 1541 Notes (2023)).
[61] Proclamation No. 7463, 66 Fed. Reg. 48197-48199, Sept. 18, 2001

has declared war or a national emergency to meet a threat to the national security of the United States. Under this statutory authority, unlimited numbers of Reservists and National Guard personnel may be called to active duty. Activation is limited to the duration of the war or the national emergency plus six months thereafter. This authority was last used on June 5, 1942, during WW II (then Title 10 U.S.C. § 672).[62]

Title 10 U.S.C. 12302(a): "Partial Mobilization" of only the Ready Reserve (Selected Reserve and Individual Ready Reserve) may be ordered to active duty by a Service Secretary IAW Title 10 U.S.C. § 12302(a), but only after the President has issued a NED and specified in the NED or a subsequent executive order the activation of this authority.[63] The Selected Reserve is composed of Troop Program Units (TPU), which includes all drilling/annual training Reserve and National Guard units; Active Guard and Reserve (AGR); and Individual Mobilization Augmentee (IMA). The President, pursuant to his authority under Title 50 U.S.C. § 1601, *et. seq.*, may declare a "national emergency" to meet any national crisis, including initiation of HD operations. Thereafter, the President may, under Title 10 U.S.C. § 12302(a), authorize the SecDef or his designated Service Secretary to involuntarily activate up to 1,000,000 Ready Reservists for up to 24 "consecutive" months. However, "consecutive" is interpreted by DoD to mean "cumulative" and may be served at different times over a period of years, but the total number of months cannot exceed 24 months for a singular declared national emergency.[64] Accordingly, a member of the Ready Reserve who has been released from active duty prior to 24 months of service under this authority, may again be involuntarily ordered back to active duty under this authority as long as the total of the combined periods of service does not exceed 24 months.

The President must report to Congress every six months explaining why continued activation is necessary. This authority was invoked by President George W. Bush as a result of the 9/11 NED on September 14, 2001, that provided Selected Reserve forces for the Gulf War between Iraq and a 42-country coalition led by the U.S.[65] More recently, President Donald Trump issued a NED for the emergency along the Southwest Border (SWB) on February 15, 2019 that included authority for the SecDef to use section 12302(a) to mobilize National Guard Soldiers and units to secure the Southwest Border (SWB) in support of Customs and Border Protection.[66] When this NED was cancelled by President Joseph Biden on 20 January 2021, DoD relied on the NED President Trump declared on 13 March 2020 for the COVID-19 emergency to continue to use section 12302(a) to call National Guard Soldiers to active duty for the SWB mission.[67] When Congress by Joint Resolution and President Biden cancelled the COVID-19 NED on 10 April 2023, DoD then relied on the NED President Biden issued

---

[62] CRS Report RL3113, *supra* note 28 at Appendix A.

[63] 50 U.S.C. § 1631 (2023).

[64] OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF THE ARMY, G-1 MOBILIZATION ROUND TABLE DISCUSSION ISSUES, DAJA-AL 2002/0238 (2002).

[65] Exec. Order No. 13,223, 66 Fed. Reg. 48,201 (Sep. 14, 2001).

[66] Proclamation 9844, 84 Fed. Reg. 4949 (Feb 15, 2019) and CDRUSNORTHCOM FRAGO 139.000 to OPORD 01-17 (FY2021 DOD Southwest Border Support to DHS), 032107ZSEP20 (UNCLASSIFIED).

[67] Proclamation 9994, 86 Fed. Reg. 15337 (Mar 13, 2020).

on 15 December 2021 against the Global Illicit Drug Trade to continue the use of section 12302(a) authority.[68] NEDs are valid for one year, unless renewed or cancelled by the President or by a Joint Resolution by Congress.[69] President Biden renewed the NED on the Global Illicit Drug Trade on December 12, 2022 and again on December 13, 2023.[70]

Title 10 U.S.C. § 12304(a): When the President determines it is necessary to augment the active forces "for any named operational mission," such as Operation Atlantic Resolve in July 2023,[71] he may issue an executive order authorizing the SecDef to involuntarily call-up no more than 200,000 members of the Selected Reserve plus the Individual Ready Reserve (IRR). No more than 30,000 of the 200,000 can come from the (IRR). However, no unit or member of a Reserve Component may be called to active duty under 10 U.S.C. § 12304(a) to perform any functions under the Insurrection Act [72] or to provide assistance to Federal, State, or local governments for a serious natural or manmade disaster, accident, or catastrophe (commonly referred to as DSCA), except to respond to an emergency involving the use or threaten use of a weapon of mass destruction or a terrorist attack or threaten terrorist attack in the United States that results or could result in significant loss of life or property. Section 12304(a) authority is generally referred to as "PRC" for Presidential Reserve Call-up authority.[73] There is no requirement under this statute for a declaration of war by Congress or a national emergency by either the Congress or the President. However, there is a 365-day time limit (formerly 270 days) per individual and this period cannot be extended. The President must notify Congress within 24 hours after exercising this authority, setting forth the reasons for this call-up and describing the anticipated use of these units or members. This authority was used recently for Operation United Assistance for support related to the Ebola virus disease outbreak in West Africa in October 2014;[74] Operation Enhance DoD Counternarcotic Operation in the Western Hemisphere in April 2020;[75] and Operation Atlantic Resolve for rotational deployments of combat-credible forces to Europe to show U.S. commitment to NATO in August 2023.[76]

Recently, in passing the National Defense Authorization Act for Fiscal Year 2024, Congress amended section 12304(a) by striking out "for any named operational mission," so that it now simply reads, "when the President determines that it is necessary to augment the active duty forces," he may authorize the SecDef to order any unit or member of the Selected Reserve or any member of the IRR to active duty with the same limitations in numbers and duration as mentioned in the above paragraph.[77]

---

[68] Exec Order No 14059, 86 Fed. Reg. 71549 (Dec 15, 2021).
[69] 50 U.S.C. § 1622(a)(1) (2023).
[70] 87 Fed. Reg. 76549 (Dec 12, 2022) and 88 Fed. Reg. 86809 (Dec 13, 2023).
[71] Exec. Order No. 14,102, 88 Fed. Reg. 45,807 (Jul 13, 2023).
[72] 10 U.S.C. §§ 251-254 (2023).
[73] CHAIRMAN OF THE J. CHIEFS OF STAFF, J. PUBL'N 4-05, JOINT MOBILIZATION PLANNING, GL-6 (2018).
[74] Exec. Order No. 13,680, 79 Fed. Reg. 63,287 (Oct. 16, 2014).
[75] Exec. Order No. 13,919, 85 Fed. Reg. 26,591 (Apr. 30, 2020).
[76] Exec. Order No. 14,102, 88 Fed. Reg. 45,807 (Jul. 13, 2023).
[77] Pub. L. No. 118-31, 137 Stat. 136, sec. 1532 (December 22, 2023)(codified as amended at 10 U.S.C. § 12304(a)).

I. Mission-Specific Rules for the Use of Force for Land HD

An unsettled question is whether the Standing Rules for the Use of Force (SRUF), as is, will continue to be used by U.S. land forces on U.S. territory for land HD missions.[78] Or will the SecDef augment the SRUF with Mission-Specific rules, such as a rule against a "declared hostile force" in the homeland theater of operations to defend the sovereignty, territory, domestic population, and critical infrastructures of the United States?[79]

When DoD military forces operate in the homeland, there are significant implications that the mistakes of one Soldier can have far-reaching social, political, and operational effects. Therefore, very clear standards for the use of non-deadly and deadly force must be established and more importantly followed. Commanders have the responsibility to teach and train their units on the rules at home station, to include issuing an appropriate rules card or brochure to each Soldier, prior to deploying from home station for a land HD mission.[80]

The SRUF in Enclosures L and N to CJCSI 3121.01B, dated 13 June 2005, comply with the Fourth Amendment to the Constitution, and provides guidance on when both non-deadly and deadly force may be employed, primarily against fellow citizens. While non-deadly forces may be used to control most situations, accomplish most missions, and provide self-defense of DoD forces under most circumstances, deadly force may only be used to prevent an "imminent threat" of death or serious bodily harm. This constitutional limitation applies to all DoD personnel performing any type of mission on U.S. territory, to include land HD operations.[81]

On the other hand, under the international Law of Armed Conflict (LOAC) enemy combatants are lawful objects and may be targeted with deadly force at any time based on their status alone as members of a "declared hostile force."[82] There is no requirement for members of a "declared hostile force" to first demonstrate an "imminent threat" of death or serious bodily harm before deadly force may be applied against them.

To further emphasize this point, if a Mission-Specific rule augmenting the SRUF declaring identifiable military forces of another country in the homeland as hostile is approved by the SecDef, then DoD forces need not follow the SRUF legal requirement for an "imminent threat" of death or serious bodily harm by enemy personnel before applying deadly force against them. It is the enemy's sole status as members of a "declared hostile force" that provides the lawful basis for targeting them immediately on sight.[83] All members of the "declared hostile force" are legitimate targets, except for medical personnel, chaplains, EPWs, wounded and shipwrecked, parachutists escaping

---

[78] JOINT CHIEFS OF STAFF, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR US FORCES, Encl. L, para. 1a (13 Jun. 2005). [hereinafter CJCSI 3121.01B].

[79] *Id.* at Encl. A, App. A, para. 1.

[80] *Id.* at Encl. A, para. 1(b); *Id.* at Encl. L, para. 1(c).

[81] *Id.* at Encl. L, para. 1(a); *Id.* at Encl. L, para. 5(c).

[82] John Cherry and Michael Rizzotti, *Understanding Self-Defense and the Law of Armed Conflict,* ARTICLES OF WAR (Mar. 9, 2021), https://lieber.westpoint.edu/understanding-self-defense-law-armed-conflict/.

[83] CJCSI 3121.01B, *supra* note 77, Encl. A, para. 2(b).

disabled aircraft, and civilians who by their conduct are not directly participating in hostilities.[84]

However, having a "declared hostile force" operating in the homeland has its ramifications. This would mean any member of the designated hostile force who committed belligerent acts in compliance with LOAC would be considered a lawful combatant for purposes of qualifying for combatant immunity. They would therefore be subject to capture and detention by DoD forces as an EPW. Otherwise, they could be considered unlawful combatants/criminals subject to arrest, detention, and trial by the Department of Justice.[85]

All DoD personnel should be reminded to immediately report any violation of or non-compliance with the applicable rules for the use of force to their commander. Commanders who receive a report of a violation of or non-compliance with the rules should conduct a preliminary inquiry to determine whether a violation or non-compliance occurred and, if so, to preserve the evidence. Commanders must immediately report suspected violations/non-compliance thru the chain of command to the Combatant Commander, ATTN: SJA.[86]

J. Levels of Detention Operations for EPWs

Engaging a "declared hostile force" in the homeland would potentially and quickly result in the capture of EPWs that would require the implementation of detention operations (DETOPS). Because DETOPS can become a sensitive matter of both political and humanitarian concerns, JAs must be prepared to advise commanders how to plan, train for, and avoid potential LOAC violations related to the treatment and classification of detainees. Additionally, JAs can expect to serve as the Recorder on Article 5 (combatant status review) and Civilian Internee Review tribunals, and perform liaison duties to the International Committee of the Red Cross (ICRC), and provide advice and support at every level of DETOPS.[87] Three DETOPS challenges to consider are: (1) the number of detainees captured, processed, and detained for long periods of time; (2) the geographic placement of detention facilities; and (3) the logistics of processing and sustaining detainees at each of the three detention levels - Detainee Collection Point (DCP), Detainee Holding Area (DHA), and Theater Detention Facility (TDF).[88] The Combatant Commander ultimately is responsible for DETOPS.[89]

---

[84] *See generally*, Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts art. 42, Jun. 8, 1977, 1125 U.N.T.S. 22.

[85] Geneva Convention Relative to the Treatment of Prisoners of War art. 5, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

[86] DEP'T OF DEFENSE, DIR. 2311.01, DOD LAW OF WAR PROGRAM 12 (2 Jul. 2020).

[87] FIELD MANUAL 3-63, *Detainee Operations,* paragraphs 1-46, 1-53, and 2-96 (Jan 2020).

[88] Major Edward Faiello and Captain Brian McCracken, "Detainee Operations: Transition from Counter-Insurgency to Large-Scale Combat Operations," *The National Security Law Quarterly,* Volume 23-4, pages 16-22, 27 November 2023.

[89] DEP'T OF DEFENSE, DIR. 2310.01E, *DoD Detainee Program,* para. 2.9 (Mar 15, 2022).

DCPs are the first line of detention beyond the Point of Capture (POC) and are typically located within a Brigade Combat Team (BCT) footprint. A Military Police (MP) platoon normally operates a DCP along with a limited number of Military Intelligence (MI) and medical personnel assigned to the BCT. The MP platoon leader is responsible for the humane treatment, evacuation, and custody and control of detainees, and the security and operation of the DCP. Emergency medical services should be provided along with sufficient food, water, and latrine facilities. Medical and administrative processing begins at the DCP, which builds on the Five Ss and T technique (search, silence, segregate, safeguard, speed to the rear, and tag) initially employed at the POC. Initial intelligence and counterintelligence collection is either limited to Tactical Questioning (TQ) by Soldiers who first encounter detainees or screening and interrogation by trained and certified MI personnel. If a detainee has not been issued an Internment Serial Number (ISN) at the POC, required within 14 days of capture, an ISN will be issued immediately and reported to the ICRC, and then used for accountability, medical records annotations, and security of any personal property purposes.[90]

Many of the challenges experienced at the DCP level will be reflected on a larger scale at the DHA where there is a 14-day detention limit. One or more DHAs should be established within the division or corps AO and preferably located adjacent to main transportation arteries to expedite further movement requirements. One MP company as well as MI and medical detachments from the division or corps typically operate a DHA. DHAs can offer additional medical care beyond emergency services, based on the availability of resources, as well as basic hygiene and food. Intelligence interrogators can assist in the decision on a detainee's status and whether to release or detain. If the decision is to detain the person, arrangements are then made to move the detainee to a TDF for more formal processing into the Detainee Reporting System (DRS), which tracks each detainee from the beginning to the termination of detention.[91]

Each TDF must satisfy minimum quality standards under both Field Manual (FM) 3-63 and international law by providing preventative medical care, hygienic and permanent housing, protection from environmental hazards, clothing and bedding, protection from public curiosity, recreation, and unfettered access by the ICRC. EPWs at the TDF are entitled to send and receive correspondence under the Geneva Convention Relative to the Treatment of Prisoners of War (GCIII). Commanders will need to decide whether this entitlement includes access to modern technology such as email and/or cell phones.[92]

Logistically, enough food, water, medical, and hygiene resources will need to be provided to every TDF to sustain an expected mass detainee population, especially

---

[90] FIELD MANUAL 3-63, *supra* note 86, Chapter 4, para 4-1 through 4-18 (January 2020).

[91] FIELD MANUAL 3-63, *supra* note 86, Chapter 4, paras 4-19 through 4-38.

[92] Major Edward Faiello and Captain Brian McCracken, "Detainee Operations: Transition from Counter-Insurgency to Large-Scale Combat Operations," *The National Security Law Quarterly,* Volume 23-4, pages 16-22, 27 November 2023.

since there will be increased scrutiny of conditions at TDFs by organizations like the ICRC. Given the need to limit population pressures on detention facilities, it will be crucial to determine the proper basis for detaining individuals by the time they reach the TDF. Under GCIII, if an individual's status is in doubt, the detaining power must treat that individual as an EPW and conduct an Article 5 tribunal, preferably with a JA as the Recorder, to determine whether the detainee meets the definition of EPW in Article 4 of the GCIII.[93]

The Geneva Conventions (GC) require specific treatment of detainees based on their status as EPW, unprivileged combatants, retained personnel, or civilians. Because hostilities in the homeland would involve the engagement of two or more countries' militaries, it would qualify as a Common Article 2 International Armed Conflict (IAC). However, Common Article 3 may still be relevant, since it requires baseline humane treatment for all detainees, even if they do not qualify as EPW, retained personnel (medical or religious military personnel), or civilians. The terms EPW and Unprivileged Enemy Belligerents (UEBs) are used to distinguish between privileged combatants entitled to additional protections under GCIII and unprivileged combatants only entitled to humane treatment under Common Article 3. It will be crucial to assess in advance how certain groups will be categorized, detained, and ultimately disposed in future hostilities, whether that disposition be by repatriation, release, or prosecution.[94]

Commanders must plan to operate DETOPS facilities and determine whether the number of facilities will stretch available MP resources. Arguably, currently there are not enough 31Es, corrections/detention specialists, to perform DETOPS. Units whose military occupation specialties (MOS) are not focused on DETOPS may need to be designated and trained on DETOPS basics pre-deployment. Such training will need to be conducted by JAs and include the LOAC and the Geneva Conventions, initial processing, and categorization, the Five Ss and T technique, TQ, the basics of establishing and guarding a DCP, Common Article 3 humane treatment, segregation, and the respective entitlements of different types of detainees. Finally, these units will need to understand the difference between TQ and interrogation, as the former is basic initial questioning for information of immediate tactical value, while the latter is a strictly regulated practice that can only be conducted by individuals who have received training under FM 2-22.3, Human Intelligence Collector Operations.

Ultimately, detainees must be classified correctly, protected, and provided certain services based on their status. Failure to comply with both Army doctrine and international law in this regard will jeopardize the military's mission and prestige, just as past failures at the Abu Ghraib prison complex in Iraq demonstrated in 2003.[95]

---

[93] *Id.*

[94] *Id*.

[95] Jeffrey F. Addicott, *Military Justice at Abu Ghraib*, JURIST (Sept. 28, 2005).

K. The Posse Comitatus Act (PCA) and HD

The PCA prohibits DoD personnel from performing direct, active law enforcement functions in civilian communities and is applicable to any active duty military personnel serving in a Title 10 capacity in the Army, Air Force, Navy, Marine Corps, and Space Force.[96] Such military personnel cannot perform direct, active law enforcement functions, such as arrests, apprehension, evidence collection, interrogation, search, security patrols, seizure, stop and frisk, surveillance, crowd control, traffic control, or other similar police functions, for or with Federal, State, or local law enforcement authorities.[97] The PCA prevents DoD personnel from performing any of the law enforcement functions described above, unless the President invokes a constitutional exception pursuant to his authority under Articles II or IV of the Constitution or an Act of Congress exception applies.[98]

Under Article II of the Constitution, the President is given the authority, as the Commander in Chief of the Armed Forces of the United States and of the militia of the several States when called into the actual service of the United States, over all military forces. He must fulfill the Constitutional responsibilities of the chief executive. Article IV, Section 4 of the Constitution also requires the United States to protect the States from invasion and, upon a request from the States, from domestic violence. Although Article II provides much of the basis for the present-day power of the President, the scope of his authority is much broader than is indicated by the rudimentary sections of this Article. Given the central role of the President, he enjoys certain implied authority to exercise inherent powers derived not from specific constitutional provisions, but from the aggregate of presidential responsibilities as the Nation's Chief Executive and Commander in Chief of the Armed Forces, and the responsibility to "take Care that the Laws be faithfully executed" under Section III of Article II.[99]

Title 6 U.S.C. § 466a (4) explains more clearly the constitutional exception to the PCA as follows: when ". . . the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection, or other serious emergency." Depending on the circumstances, HD could be included "in time of war" or "other serious emergency" as a constitutional exception to the PCA. Thus, if the President invokes this authority, military commanders may then order, and unit personnel may then perform law enforcement functions, respectively, when conducting land HD missions "in time of war" or "other serious emergency," if necessary, to accomplish their unit's mission successfully.[100]

---

[96] 18 U.S.C. §1385 (2023).

[97] DEP'T OF DEFENSE, INSTR. 3025.21, DEFENSE SUPPORT OF CIVILIAN LAW ENFORCEMENT AGENCIES 16 – 25 (27 Feb. 2013) (Ch. 1, 8 Feb. 2019) [hereinafter DODI 3025.21].

[98] 6 U.S.C. § 466a(4) (2023).

[99] MARTIN SHAPIRO & ROCCO J. TRESOLINI, AMERICAN CONSTITUTIONAL LAW 164 – 73 (4th ed. 1979).

[100] JP 3-27, *supra* note 1, I-7.

L. Protection of Defense Critical Infrastructures (DCI) and Other Designated Properties

Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, supersedes Homeland Security Presidential Directive 7 and advances a National policy to strengthen and maintain secure, functioning, and resilient critical infrastructures.[101] This directive identifies 16 critical infrastructure sectors (CIS) whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, National economic security, National public health or safety, or any combination thereof. DoD is responsible for only one CIS - the Defense Industrial Base (DIB), which can be expected to be targeted first by the enemy.[102]

Beginning in 2006, the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs (ASD(HD&ASA) (now Homeland Defense and Hemispheric Affairs (HD&HA)) (See paragraph F above) collaborated with the Joint Staff to compile a SECRET list of all DoD- and non-DoD-owned defense critical infrastructures (DCI) essential to DoD's ability to deploy, support, and sustain forces and operations worldwide and to implement its core missions. To support this effort, the combatant commands and military services identified and characterize their critical infrastructures based on mission impact and prioritized them into three tiers. Tier 1 Task Critical Assets (TCA) are assets whose loss, incapacitation, or disruption would result in mission failure at the DoD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level. Tier 2 TCA are assets the loss, incapacitation, or disruption of which would result in severe mission degradation at the DoD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level. Tier 3 TCA are assets the loss, incapacitation, or disruption of which would result in mission failure below the military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level. Then in 2008, the ASD(HD&ASA) accepted the Joint Staff's recommendation for an initial Defense Critical Assets (DCA) list from the hundreds of Tiers 1 TCA, which are those assets of such extraordinary importance to operations in peace, crisis, and war that their incapacitation or destruction would have a very serious debilitating effect on the ability of DoD to fulfill its missions. The DCA list is classified TOP SECRET.[103] The DCA list is updated and validated by the Joint Staff and approved by the SecDef annually.[104]

DoDD 3020.40 directs Combatant Commanders to ensure DoD can execute HD missions by preventing or mitigating the loss or degradation of DoD-owned DCI within

---

[101] Presidential Policy Directive – 21, *Critical Infrastructure Security and Resilience* (Feb 12, 2013).

[102] *Id.* at 11.

[103] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-740R, DEFENSE CRITICAL INFRASTRUCTURE: ACTIONS NEEDED TO IMPROVE THE CONSISTENCY, RELIABILITY, AND USEFULNESS OF DOD'S TIER 1 TASK CRITICAL ASSET LIST 1 – 2 (2009).

[104] DoD HOMELAND DEFENSE POLICY GUIDANCE, *supra* note 4, at 5.

an assigned AOR in coordination with the asset owner.[105] CDRUSNORTHCOM has no responsibility to prevent or mitigate the loss or degradation of non-DoD-owned DCI within the NORTHCOM AOR; instead, that statutory mission belongs to the Department of Homeland Security (DHS).[106] Although the CDRUSNORTHCOM has the responsibility to address the protection and mission assurance of DoD-owned DCI in his geographical area, he has no assigned forces designated to perform this specific protection mission.[107] In order for the Joint Staff to allocate additional forces to NORTHCOM to fill this gap, the CDRUSNORTHCOM must submit a Request for Forces (RFF) to the SecDef for this capability.[108] Once the requested forces are provided to NORTHCOM by a force provider, NORTHCOM will delegate command authority to ARNORTH as the Theater JFLCC to perform the DCI protection mission.[109]

In performing its DoDD 3020.40 responsibilities, the CDRUSNORTHCOM established a Defended Assets List (DAL) classified at the SECRET level containing those assets on the Critical Assets List (CAL) in the NORTHCOM AOR that must be defended by the JFLCC's air and missile defense (AMD) capabilities.[110] Changes to the DAL can be anticipated with changes in the priority of defended assets, loss of AMD assets, inventory depletion, or the arrival of additional AMD forces.[111]

CJCSI 3121.01B provides another category that includes four types of special "designated" properties that may require military forces to protect them with force, to include deadly force. First, the President may designate any critical infrastructure as a National Critical Infrastructure (NCI). These are public utilities or similar critical infrastructures vital to public health or safety e.g. power plants, dams, water treatment plants, oil pipelines, the damage to which the President has determined would create an imminent threat of death or serious bodily harm to the population.[112]

Second, the President may designate any very sensitive strategic asset as an Asset Vital to National Security (AVNS). These DoD and non-DoD properties may include, but are not limited to nuclear weapons, nuclear C2 facilities, restrictive areas containing strategic operational assets, sensitive codes or special access programs, key civilian and military transportation nodes the actual theft or sabotage of which the President has determined would seriously jeopardize the fulfillment of a national defense mission and would create an imminent threat of death or serious bodily harm to the population.[113]

---

[105] DEP'T OF DEFENSE, DIR. 3020.40, MISSION ASSURANCE 12 (NOV. 29, 2016) (Ch. 1, Sep. 11, 2018) [hereinafter DoDD 3020.40].

[106] 6 U.S.C. §§ 671-674 (2023).

[107] DEP'T OF DEFENSE, INSTR. 2000.12, DOD ANTITERRORISM (AT) PROGRAM, Encl. 2, para. 18(h) (Mar. 1, 2012) (Ch. 3, May 8, 2017).

[108] JOINT CHIEFS OF STAFF, CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL 3130.06C, GLOBAL FORCE MANAGEMENT (GFM) ALLOCATION POLICIES AND PROCEDURES, ENCL. C (7 May. 2021). [hereinafter CJCSM 3130.06C].

[109] JOINT CHIEFS OF STAFF, J. PUBL'N 3-0, JOINT CAMPAIGNS AND OPERATIONS, III-3, FIGURE III-1 (JUN 18, 2022).

[110] JOINT CHIEFS OF STAFF, J. PUBL'N 3-01, COUNTERING AIR AND MISSILE THREATS, III-16, para. 16(b) (Apr. 6, 2023).

[111] *Id. at* III-19, para. 18(b).

[112] CJCSI 3121.01B*, supra* note 77, Encl L, para 4(g).

[113] *Id.* at Encl. L, para. 4(e)

Once a critical infrastructure is designated as an NCI or a strategic asset is designated as an AVNS, it is treated as federal property for protection purposes. The President has the constitutional duty to protect federal property and the inherent authority to use military forces to perform this protection mission.[114]

Third, Inherently Dangerous Property (IDP) is property designated by the on-scene commander and not limited to: weapons, ammo, grenades, explosives, portable missiles, rockets, chemical agents, special nuclear materials, and other movable armaments and ordnances that if in the hands of an unauthorized individual, the on-scene commander has determined would create an imminent threat of death or serious bodily harm to the installation and its personnel.[115]

Fourth, Enclosure I to CJCSI 3121.01B, provides a list of numbered Supplemental Measures to the Standing Rules of Engagement (SROE), classified at the CONFIDENTIAL level. These Supplemental Measures are intended to be used outside U.S. territory against an enemy force to enable commanders to appropriately address unforeseen situations when immediate decisions and responses are required.[116] Supplemental Measure 504 pertains to "mission essential property" (MEP) that allows any commander to independently define and then protect with deadly force, if necessary, unless this authority is withheld by the CCDR.[117] If the SecDef approves Supplemental Measure 504 as a Mission-Specific RUF for use in the homeland, it could be used as authority to protect other property that is essential to a HD mission, such as in a "fort-to-port" scenario. A commander could determine that a critical piece of non-DoD property along the route, such as a bridge, is so significant that its loss or damage would result in mission failure at the combatant command level to project combat power around the world successfully and would create an imminent threat of death or serious bodily harm to U.S. forces if the property was damaged or destroyed. The commander could designate the bridge as "mission essential property," which would convert it to DoD property for protection purposes. The commander would then have the inherent responsibility to protect it against any threat of damage or destruction with his forces.

According to the DoD/DHS DIB Defense Plan, May 2010, the following protection principles of layered defense apply to DIB critical assets:

(1) First level of protection: Asset owners are responsible for providing the first level of protection with either DoD or contract security personnel.

(2) Second level of protection: As the seriousness of threats escalates, local law enforcement authorities will assist the asset owner in meeting protective responsibilities.

---

[114] AUTHORITY TO USE TROOPS TO PROTECT FEDERAL FUNCTIONS, INCLUDING THE SAFEGUARDING OF FOREIGN EMBASSIES IN THE UNITED STATES, OFFICE OF LEGAL COUNSEL, U.S. DEP'T OF JUSTICE (May 11, 1970) and title 6 U.S.C § 466(a)(4).

[115] CJCSI 3121.01B, *supra* note 77, Encl. L, para 4(f).

[116] *Id. at Encl* I, pg. 2.

[117] *Id*.

(3) Third level of protection: If the response from local authorities does not provide the necessary level of protection, State and/or Federal civil law enforcement authorities can be employed to provide additional security capability.

(4) Fourth level of protection: In more serious situations, a State Governor may employ the National Guard under his or her command and control in either a State Active Duty (SAD) or Title 32 status pursuant to Title 32 U.S.C. Chapter 9.

(5) Fifth level of protection: As a last resort and only when warranted, the President may direct the employment of DoD forces in a Title 10 status to protect threatened DIB assets.[118]

IAW the DoD/DHS DIB Defense Plan, DoD forces are the option of last resort for the protection of a DIB infrastructure. Of the many lists and designations of critical infrastructures in the 16 CIS, including the DIB, protection priority will be based on (1) the infrastructure's criticality to mission execution, (2) existing threats to the infrastructure, and (3) the infrastructure's vulnerabilities.[119] However, DoD commanders must be prepared to adjust their internal protection priorities of DIB and DCIs to those infrastructures and assets the President designates as either an NCI or AVNS, respectively.

M. Confiscation of Private Property for HD

Army Regulation (AR) 405-10 provides an overview of the process by which the Department of the Army (DA) acquires non-Federal property for military purposes. As a threshold issue, this regulation recognizes that although "the Federal Government has the inherent power to acquire land for its constitutional purposes, this power can be exercised only at the discretion of Congress." As such, the acquisition of non-Federal property must be "expressly authorized by law."[120]

In 1956, Congress enacted such a law in Title 10 U.S.C. § 2663. This statute provides the military departments with the authorization to acquire land "in time of war or when war is imminent" and where the Secretary of the Army determines that the land is "needed in the interest of national defense."[121] The HQDA could pursue such an acquisition, to include by gift, purchase, exchange of real property owned by the United States or, in extreme cases, through condemnation proceedings in U.S. District Court.[122] Although generally the Secretary of the Army must pursue "all other available

[118] DEP'T OF DEFENSE & DEP'T OF HOMELAND SECURITY, DEFENSE INDUSTRIAL BASE SECTOR-SPECIFIC PLAN: AN ANNEX TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN, 37-38 (2010).
[119] DoDD 3020.40, *supra* note 104, pg. 15 para. 3.2.
[120] U.S. ARMY, REGULATION 405-10, ACQUISITION OF REAL PROPERTY AND INTERESTS THEREIN, para. 1-3, (1 Aug. 1970) [hereinafter AR 405-10].
[121] 10 U.S.C. § 2663(a)(2) (2023); 10 U.S.C. §2663(d)(1)(A) (2023).
[122] 10 U.S.C. § 2663(e) (2023).

options for the acquisition of land," and must wait 21 days after reporting the intent to acquire the land through condemnation proceedings, no such report or accompanying waiting period is required if the taking of the land in question is "vital to national security" and "delay would be detrimental to national security." In these instances, the Secretary of the Army is only required to report to Congress within seven days after commencement of the condemnation proceedings.[123]

Prior to pursuing any course of action involving non-Federal property acquisition, AR 405-10 requires a determination that: (1) the activity to be accommodated is essential to an assigned mission; (2) real property under the control of the Army is inadequate to satisfy the requirement; and (3) no real property under the control of the Navy or Air Force or other Federal agency is suitable and available for use by the Army on a permit or joint use basis.[124]

Once these determinations have been made, the next step is to contact the U.S. Army Corps of Engineers. Army Regulation 405-10, paragraph 2-9 makes the U.S. Army Corps of Engineers (USACE) the real estate executive agent for the Army. The USACE liaison officer to ARNORTH will begin the process of coordination for obtaining the required land through USACE channels. USACE will evaluate the proposed property for site selection and suitability, research and determine ownership, calculate the estimated fair market value for the desired ownership interest, and, if time and circumstances permit, negotiate with the owner for lease or purchase of the land.[125]

In 2006, Congress, in John Warner National Defense Authorization Act Fiscal Year 2007, issued a Sense of Congress statement indicating that: "the Secretary of Defense, when acquiring land for military purposes should (1) make every effort to acquire land by means of purchases from willing sellers; and (2) employ condemnation, eminent domain, or seizure procedures *only as a measure of last resort* in cases of *compelling national security requirements* or at the request of the seller."[126]

When the USACE team is unable to reach an agreement with the property owner, or title defects do not permit acquisition by lease or purchase, or time constraints do not allow USACE sufficient time to conduct normal negotiations, then "fee title, easements, or leasehold interest may be acquired by the exercise of the right of eminent domain through the institution of condemnation proceedings."[127] In these instances, the Secretary of the Army, when prompted by the USACE Chief of Engineers, would request the Attorney General to file condemnation proceedings in the U.S. District Court that has jurisdiction over the property. Generally, the court has discretion regarding the time needed to determine, among other things, the fair market value of the property,

---

[123] 10 U.S.C. § 2663(g) (2023).
[124] AR 405-10, *supra* note 119, para. 1-5(a).
[125] *Id.*
[126] John Warner National Defense Authorization Act Fiscal Year 2007, Pub. L. No. 109-364, 120 Stat. 2085 (2006) [hereinafter FY07 NDAA].
[127] AR 405-10, *supra* note 119, para. 2-9j (1).

and the time and terms of the DoD possession of the property. In time of war, however, the Attorney General can file a Request for an Order of Immediate Possession, allowing immediate possession for military and national defense purposes.[128]

N. Quick Response Force/Rapid Response Force (QRF/RRF) for HD

Pursuant to his authority under Article II of the Constitution as the Commander in Chief and his inherent powers as the Nation's Chief Executive, the President may direct the deployment of forces to reinforce the security posture at DoD installations, to protect Presidential-designated assets and infrastructures, or to conduct a show of force as a deterrence to attack.[129] These units are referred to as the Quick Response Force/Rapid Response Force; QRF is a company size unit and the RRF is battalion size with three QRFs.[130] The SecDef is the approval authority for all QRF/RRF missions, deployments, and employments.[131] CDRUSNORTHCOM and CDRINDOPACOM) are the Supported Combatant Commanders for land HD operations within their respective AOR.[132]

Altogether, nine RRFs are authorized and located throughout the USNORTHCOM and USINDOPACOM AORs and, if necessary, could fall under an allocated brigade headquarters for land HD missions.[133] The identity of pre-designated units, plus their exact composition, the precise nature of their deployment/employment mission, and the tiered response posture levels are classified SECRET//REL USA AND FIVE EYES.[134]

The concept is to maintain a tiered response system, that supports the rapid deployment of the QRF/RRF in response to domestic threats consistent with U.S. law and DoD policy.[135] Forces deploy with inherent force protection capability and may be deployed to secure/defend a single site or multiple sites.[136]

There are two sets of Rules for the Use of Force (RUF) that apply to QRF/RRF operations. One is not widely known and is provided by CJCS message subject: RUF for QRF/RRF Ground Security, dated 072310 August 2003, and the other is provided in Enclosures L and N to CJCSI 3121.01B, dated 13 June 2005, and is commonly referred to as the SRUF. Which set of RUF applies to a given situation will depend on the intended location for the QRF/RRF mission.[137]

---

[128] AR 405-10, *supra* note 119, para. 2-9j (3).

[129] Forces Command (FORSCOM) EXORD ISO Homeland Defense FY23, para.1. D.1.A. (UNCLASSIFIED), 281400ZJUL22 (SECRET). [hereinafter 23 FORSCOM HD EXORD).

[130] JS HQ EXORD, *supra* note 23, para. 3.A.1.A - 3.A.1.C. (U).

[131] *Id.* at para. 3.A.1.(U).

[132] *Id.* at para. 11.A.1.(U).

[133] *Id.* at para. 3.A.1.D. (U).

[134] *Id.* at para. 9 (U).

[135] 23 FORSCOM HD EXORD, *supra* note 128, para. 3.A.5.A. (U).

[136] JS HD EXORD, *supra* note 23, para. 3.A.1.A. (U).

[137] Joint Staff message for Rules for the Use of Force (RUF) for QRF/RRF Ground Security Operations, para. 1, 072310ZAUG03 (SECRET//REL TO USA AND CAN) [hereinafter QRF/RRF RUF].

Except for one difference, these two sets of RUF are similar and should be used for training as well as operational purposes. The difference concerns going to the defense of non-DoD personnel in the vicinity. The SRUF limits non-QRF/RRF forces going to the defense of non-DoD personnel in the vicinity to only when doing so is "directly related to the assigned mission."[138] The "assigned mission" is the same as paragraph 2 of the unit's operations order (OPORD). There is no such restriction in the QRF/RRF ground security RUF. Regardless of which RUF will initially apply, it will remain in effect until mission specific RUF is approved by the SecDef.[139]

QRF/RRF forces will deploy armed. The SecDef will authorize QRF/RRF forces to deploy with and carry individual weapons during the QRF/RRF mission. The SecDef designates CDRUSNORTHCOM as weapons "loading" authority. CDRUSNORTHCOM may delegate this authority to the CDRUSARNORTH, or to a JTF commander, or to the QRF/RRF unit commander, or to a regional Defense Coordinating Officer.[140]

O. Chemical, Biological, Radiological or Nuclear (CBRN) Response Force for HD

Beginning in 1996, Congress tasked DoD to develop and maintain the capability to detect, neutralize, contain, dismantle, and dispose of weapons of mass destruction that contained chemical, biological, or "related materials."[141] In 2006, Congress changed "related materials" to "radiological, nuclear, and high-yield explosives."[142] By 2009, DoD was prepared to provide CBRN response support for three nearly-simultaneous, geographically dispersed, significant CBRN incidents or one catastrophic CBRN incident.[143] This response capability was called the DoD CBRN Response Enterprise, otherwise referred to as the CRE.[144] It is the set of forces DoD has sourced to defend the homeland by being ready to deploy anywhere in the U.S. to respond to "America's Worst Day."[145] This set of forces is composed of active-duty, Reserve, and National Guard units. CDRUSNORTHCOM and CDRINDOPACOM are responsible for employing and directing federal CBRN response forces in their respective AOR through 31 May 2025.[146] Governors are responsible for ordering and directing National Guard forces who are in a Title 32 or SAD status.[147]

---

[138] CJCSI 3121.01B, *supra* note 77, Encl. L, paras. 5b (1), 5(c)2, and 5d; *Id.* Encl. N, paras 4b(1)(c) and 4d.
[139] QRF/RRF RUF, *supra* note 136, para. 7 (U).
[140] *Id.* at para. 6C (U).
[141] Pub. L. No. 104-201, 110 Stat.2720, sec. 1414(a) (codified as amended at 50 U.S.C. §2314(2023)).
[142] 50 U.S.C. § 2314 (2023).
[143] JOINT CHIEFS OF STAFF, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTR. 3125.01B, DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) FOR DEFENSE CONSEQUENCE MANAGEMENT OPERATIONS IN RESPONSE TO A CBRN INCIDENT, Encl. L, para. 1a (19 Aug. 2009). [hereinafter CJCSI 3125.01B].
[144] Joint Staff Domestic CBRN Response EXORD (CUI), 241452ZMAR16, para. 1.B.1. (UNCLASSIFIED) [hereinafter CBRN Response EXORD].
[145] JOINT CHIEFS OF STAFF, J. PUBL'N 3-41, CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR RESPONSE, I-3 (9 DECEMBER 2016) [hereinafter JP 3-41].
[146] *Id.* at para. 1.D (U).
[147] *Id.* at para. 5.A.3 (U).

The employment of the CRE is a graduated or tiered response construct. The larger the CBRN event, the greater the number of CRE units that will be deployed to respond. National Guard forces are programmed as the first responders.[148] Federal forces, both active duty and Reserve, are programmed to respond if additional capabilities are required.[149]

The National Guard forces include (1) 57 Weapons of Mass Destruction Civil Support Teams (WMD-CST), (2) 17 CBRN Enhanced Response Force Package (CERFP), and (3) 10 Homeland Response Force (HRF).[150]

The WMD-CSTs are a creature of statute and are the first tier in the DoD CRE.[151] Every State and territory has at least one WMD-CST. California, New York, and Florida have two WMD-CSTs. These units are composed of 22 National Guard Soldiers in a full-time Title 32 status. It must be prepared to deploy within three hours of notification by a proper State authority to identify the CBRN material, assess the consequences, and advise civil authorities on appropriate response measures.[152]

The CERFPs are the second tier in the DoD CBRN Response Enterprise. It is a 186-member National Guard organization postured in 17 States. A CERFP must be prepared to deploy within six hours of notification to provide search and extraction, decontamination, and emergency medical capabilities. It deploys in a SAD status.[153]

The HRFs are the third tier in the DoD CBRN Response Enterprise. It will also deploy in a SAD status. They are a 560-member National Guard organization, one located in each of the ten FEMA regions. Each HRF must be prepared to deploy within 12 hours of notification to provide Command and Control (C2), CBRN assessment, search & extraction, decontamination, emergency medical, and security capabilities.[154]

Federal forces in a Title 10 active-duty status are composed of the three two-star headquarters: (1) Defense CBRN Response Force (DCRF), (2) Command and Control CBRN Response Element Alpha (C2CRE-A), and (3) Command and Control CBRN Response Element Bravo (C2CRE-B).[155] These three units would satisfy the DoD requirement to respond to three nearly-simultaneous, geographically dispersed CBRN events in the homeland.

The DCRF is Joint Task Force-Civil Support (JTF-CS) with three brigade task forces (Operations, Medical, and Aviation).[156] It provides the fourth tier in the DoD CBRN

---

[148] *Id.* at para. 1.C.1 (U).
[149] *Id.* at para. 3.A.1 (U).
[150] *Id.* at para. 1.B.1.A (U).
[151] 10 U.S.C. § 12310(c); FY07 NDAA, *supra* note 125, sec. 527; National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, sec. 1435 (2013).
[152] CBRN Response EXORD, *supra* note 143, para. 3.B.4.A (U).
[153] *Id.* at para. 3.B.4.B (U).
[154] *Id.* para. 3.B.4.C (U).
[155] *Id*. para. 1.B.1.B (U).
[156] FORSCOM EXORD ISO CBRN CRE FY24, paragraph 1.B.1, 191515ZMAY23 [hereinafter 24 FORSCOM CBRN EXORD].

Response Enterprise. It is not-to-exceed 5200-member organization composed of active-duty and Reserve Soldiers and divided into two separate force packages, FP-1 (2100) and FP-2 (3100).[157] The DCRF can provide search & extraction, decontamination, aviation, engineering, logistics, and emergency medical capabilities.[158]

C2CRE-A is the 76th Operational Response Command.[159] It provides the fifth tier in the DoD CBRN Response Enterprise. It is a not-to-exceed 1500-member organization composed of primarily Reserve units.[160] It can provide life sustaining, logistical, C2, search & rescue, chemical reconnaissance, decontamination, and emergency medical capabilities.[161]

C2CRE-B is the 46th Military Police Command in the Michigan Army National Guard.[162] It provides the sixth tier in the DoD CBRN Response Enterprise. It is also a not-to-exceed 1500-member organization composed of primarily National Guard units that will be in a Title 10 active-duty status.[163] It can provide life sustaining, logistical, C2, search & rescue, chemical reconnaissance, decontamination, and emergency medical capabilities.[164]

Federal forces will follow a graduated CBRN Response Posture Level (CRPL). CRPL-1 is Ready to deploy on notification plus 24 hours (N+24). CRPL-2 is Ready to deploy on notification plus 48 hours (N+48). CRPL-3 is Ready to deploy on notification plus 72 hours (N+72). CRPL-4 is Ready to deploy on notification plus 96 hours (N+96).[165] The Supported Combatant Commander may change the CRPL up to CRPL-1.[166]

The Supported Combatant Commander assumes Operational Control (OPCON) of forces upon arrival in the Supported Combatant Commander's Joint AOR and upon completion of the mission relinquishes OPCON upon departure from the AOR.[167] Depending on the call to active duty authority used (See paragraph I above), either SecDef or Secretary of a Military Department approval is required to call to active-duty National Guard and/or Reserve forces, except for the WMD-CSTs, into Title 10 Federal status in order to be employed by the Supported Combatant Commander.[168]

There is one other DoD organization that has the CBRN response mission. In 1995, the 31st Commandant of the Marine Corps, General Charles Krulak, provided planning guidance that identified the need for a strategic organization to respond to a growing

---

[157] CBRN Response EXORD, *supra* note 143, para. 3.B.5.A; *Id.* at para. 3.B.9.B.1.(U).
[158] 24 FORSCOM CBRN EXORD, *supra* note 155, para. 1.B.1 (U).
[159] *Id.* at para. 5.A.2.C.1 (U).
[160] *Id.* at para. 3.B.1.C (U).
[161] *Id.* at para. 1.B.2; *Id.* at para. 3.B.1.C (U).
[162] *Id.* at para. 5.A.2.C.(U).
[163] CBRN Response EXORD, *supra* note 143, para. 3.B.9.B.1 (U).
[164] 24 FORSCOM CBRN EXORD, *supra* note 155, para. 1.B.2; *Id.* at para. 3.B.1.C (U).
[165] CBRN Response EXORD, *supra* note 143, para 3.B.2 (U).
[166] *Id.* at para. 3.B.7.A.1.A (U).
[167] *Id.* at para. 3.B.7.B.8 (U).
[168] *Id.* at para. 3.B.9.B.3 (U).

chemical/biological terrorist threat. The Chemical Biological Incident Response Force (CBIRF) concept was developed by the Marine Corps Warfighting Laboratory and came to fruition in 1996. The 500-person active-duty unit is located at Naval Support Facility in Indian Head, Maryland. Less than 30 miles from the U.S. Capitol building, the CBIRF's proximity to the National Capital Region makes it the force of choice within DoD when responding to CBRN threats in Washington, D.C. The CBIRF is prepared to respond, with minimal warning, to a chemical, biological, radiological, nuclear, or high yield explosive event. As such, CBIRF Marines and Sailors are skilled in the areas of C2, agent detection and identification, search, rescue, and decontamination, and emergency medical care for contaminated personnel.[169]

The CBRN Response Enterprise is DoD's contribution to the whole of government approach for a CBRN incident response within the U.S. It now exceeds 18,000 personnel and has several specialized capabilities to meet its CJCS-mandated requirements. Priority Initiative Six of the Homeland Defense Policy Guidance emphasizes reinvigorating CBRN training in the active duty force, Reserves, and National Guard that addresses the response to attacks on the homeland that build upon lessons learned from responses to DSCA events.[170]

P. National Capitol Region-Integrated Air Defense System (NCR-IADS) for HD

DoD must focus its homeland Integrated Air Defense Systems (IADS) capabilities on the protection of the Nation against an enemy's military aircraft, both manned and unmanned, as well as missile threats to the homeland. IADS is part of joint air defense systems, both offensive and defense, whose purpose is to control the air space and destroy enemy aircraft and missiles before and after launch. Offensive counterair operations include attack operations, suppression of enemy air defenses, fighter escort, and fighter sweep. Defensive counterair operations encompasses air and missile defense taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats.[171]

An IADS is normally established for defensive counterair operations purposes. The goal of defensive counterair operations is to provide an area from which HD forces can operate while protected from air and missile threats.[172] The IADS is a robust integration of capabilities and comprises sensors, weapons, C2 systems, intelligence systems, and the personnel who operate them.[173]

The IADS for the National Capital Region (NCR) was created shortly after the September 11, 2001, terrorist attacks to provide low-altitude, low-airspeed detection

[169] https://www.cbirf.marines.mil

[170] Homeland Defense Policy Guidance, s*upra* note 4, at 20.

[171] JOINT CHIEFS OF STAFF, J. PUBL'N 3-01, COUNTERING AIR AND MISSILE THREATS, I-1, para. 1 (06 April 2023) [herein after JP 3-01].

[172] *Id.* at I-6, para. 3(c)(2).

[173] *Id.* at II-11, para. 7(b).

capabilities to defend against airborne threats to the NCR. The NCR-IADS is a component in the defense of the NCR through the coordination, cooperation and collaboration of the United States Air Force and the United States Army.[174] As an activity of the North American Aerospace Defense Command (NORAD) and the Joint Air Defense Operations Center, the NCR-IADS operates and trains throughout the NCR.[175] Units allocated to the NCR-IADS mission develop and execute core Mission Essential Task List (METL) training for follow-on missions or global contingencies.[176]

More specifically, NCR-IADS provides ground-based air defense of the NCR airspace, and provides an integrated 360-degree air picture, ground air defense weapons, enhanced regional situational awareness, and forensic data collection capabilities for the warfighter mission to protect the NCR.[177] USARNORTH has Army Service Component Command authority for the NCR-IADS units.[178] JTF-NCR is responsible for the conduct of specific operations within the NCR JOA.[179] NCR-IADS's purpose is to provide freedom of action by the U.S. government and to safeguard the continuity of daily government operations 24 hours a day, seven days a week, 365 days a year.[180]

The term "National Capital Region" means the geographic area located within the boundaries of (A) the District of Columbia, (B) Montgomery and Prince Georges Counties in the State of Maryland, (C) Arlington, Fairfax, Loudoun, and Prince William Counties and the City of Alexandria in the Commonwealth of Virginia, and (D) all cities and other units of government within the geographic areas of such District, Counties, and City.[181]

Additionally, the NCR-IADS is a statutory "covered facility or asset"[182] that the SecDef may authorize DoD personnel to protect against a threat that an unmanned aircraft system or unmanned aircraft poses to its safety or security. This includes identifying, detecting, monitoring, tracking, warning, disrupting, seizing, disabling, damaging, and destroying the aircraft.[183]

Additional operational information about the NCR-IADS is classified SECRET.

---

[174] Jessica Casserly, *Hanscom looks to modernize NCR defense system,* 66th Air Base Group Public Affairs, (9 Dec 2020).

[175] DVIDS - Images - NCR-IADS Transfer of Authority Ceremony [Image 1 of 4] (dvidshub.net)

[176] FORSCOM EXORD ISO NCR-IADS FY24, para. 3.B.2.H., 072045ZJUN23 (SECRET// REL FVEY) [hereafter FORSCOM EXORD ISO NCR-IADS FY24].

[177] NCR-IADS Exhibit P-40, Budget Line-Item Justification, Battle Control System, February 2019.

[178] FORSCOM EXORD ISO NCR-IADS FY24, *supra* note 175, para. 1.D.2.B.

[179] *Id.* at para. 1.D.2.D.

[180] SGT Brad Mincey, *263rd AAMDC validates, certifies training for NCR deployment*, U.S. ARMY (28 Jul 2016), https://www.army.mil/article/172376/263rd_aamdc_validates_certifies_training_for_ncr_deployment.

[181] 10 U.S.C. § 2674(f)(2) (2023); Title 40 U.S.C. § 8702(3) (2023).

[182] 10 U.S.C. §130i(j)(3)(C)(v).

[183] 10 U.S.C. § 130i (2023).

Q. Unmanned Aircraft Systems (UAS) and Countermeasures during HD

One of the more remarkable recent developments in the application of technology that can be used for dual civilian and military purposes has been the ever-increasing use of unmanned aircraft systems (UAS) or drones. Most recently, the use of drone warfare in conflicts between Azerbaijan and Armenia, Ukraine and Russia, or Houthi use of unmanned systems to attack maritime traffic off the coast of Yemen underscore the relevance and relative paradigm shift in air and land domain warfare. Availability and accessibility of the remotely operated aircraft technology gave rise to both new threats and new methods in conducting HD operations.

The ubiquitous presence of the UAS in the Homeland has led to the increased illicit use in criminal activities, conducting illegal surveillance and industrial espionage, or thwarting law enforcement levels at the local, state, and Federal level. In addition, UAS have been utilized by state-level actors to support global competition intelligence collection requirements, such as the recently publicized use of high-altitude balloon tethered systems with navigational and intelligence collection capabilities over U.S. territory.

This chapter sets out the foundational information considering the regulation of airspace and potential issues that can arise in HD operations seeking to counter the small UAS use. The concerns regarding the safety of the domestic air domain were addressed by the Department of Homeland Security in the National Strategy for Aviation Security, as originally published in 2007 and periodically updated through the most recent edition in 2018.[184] More specifically, to address unmanned aerial system threats in the Homeland, the Federal government issued The Domestic Counter-Unmanned Aircraft Systems (c-UAS) National Action Plan in April of 2022.[185]

The regulatory control of the air space over the Homeland is executed through the National Airspace System framework. National Airspace System (NAS) has been codified to assert the U.S. sovereignty over its airspace.[186] The United States Government has exclusive sovereignty of national airspace of the United States.[187] However, the individual rights of citizens have been set out explicitly by stating that a citizen of the United States has a public right of transit through the navigable airspace.[188] The code further defines an “aircraft” as any device used, or intended to be used, for flight, and designates the UAS as “aircraft” subject to regulation.[189] Therefore, the UAS flown outdoors operate in the National Airspace System and are subject to the U.S. Government regulation.

[184] https://www.dhs.gov/publication/national-strategy-aviation-security

[185] https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/

[186] 49 U.S.C. § 40103, Sovereignty and Use of Airspace

[187] Pursuant to 49 U.S.C. § 40103(a)(1)

[188] 49 U.S.C. § 40103(a)(2)

[189] 49 U.S.C. § 40102(a)(6), and 14 CFR § 1.1

The regulating of the national airspace is executed through the Federal Aviation Administration (FAA). It was established through the FAA Act of 1958, and further codified under Title 18 and Title 49 of the United States Code, and Title 14 of the Code of Federal Regulations. Under these federal laws, the FAA is an administrative and regulatory agency with authority over U.S. civil aviation, also vested with the authority to enforce civil penalties and certificate actions.

Since 2016, the FAA has integrated the small UAS (sUAS) into the NAS.[190] It promulgated regulations setting forth certification requirements for UAS operators, required radio frequency (RF) identification technology to be included in the UAS use, and designated specific flight zones as Class A-G airspace, depending on the altitude and land features.[191] The FAA also expanded the definition of navigable airspace to include the air space in the altitude below 500 feet above ground level, to account for the growing use of sUAS. To address immediate security concerns, the FAA promulgated safe operation guidelines, sensitive airspace restrictions, and measures to help identify such restricted areas to the UAS operators.[192]

Security Sensitive Airspace Restrictions

Drones are prohibited from flying over designated national security sensitive facilities. Operations are prohibited from the ground up to 400 feet above ground level and apply to all types and purposes of UAS flight operations. Examples of these locations are:

- Military bases designated as Department of Defense facilities
- National landmarks – Statue of Liberty, Hoover Dam, Mt. Rushmore etc.
- Certain critical infrastructure, such as nuclear power plants

The FAA has promoted the use of "No Drone Zone" signage, that can be used by government entities to identify areas where there are local restrictions.[193] It is of note that "No Drone Zones" only restrict taking off or landing in the identified zone, and do not restrict *flight* in the airspace above the identified area.

To control *flight* through restricted airspace, the FAA also uses Temporary Flight Restrictions (TFR). These define a certain area of airspace where air travel is limited for a period and may be in place for different reasons. Examples include, major sporting events, space launch and reentry operations, presidential movements, or in security sensitive areas designated by federal agencies. Restriction details of the TFR include, size, altitude, date/time, and what types of operations are restricted and permitted. All pilots are required to adhere to the restrictions of the TFR.[194] A violation of the TFR zone is a misdemeanor and carries a penalty of up to one year in prison.

[190] 14 C.F.R. § 107

[191] https://www.faa.gov/uas/getting_started/where_can_i_fly/airspace_101

[192] See id.

[193] https://www.faa.gov/uas/resources/community_engagement/no_drone_zone

[194] 49 U.S.C. § 46307

In addition to restricting flight in specified airspace, the FAA promulgates guidelines to help promote responsible UAS operation.[195] These guidelines can also be taken into consideration when analyzing the UAS flight patterns to help distinguish between lawful civilian operation and potential hostile or criminal use. Common UAS rules for Air Traffic Control coordinated use and recreational operators include:

- Do not fly over 400 feet in uncontrolled airspace
- Obtain authorization before flying in controlled airspace (Class B, C, D, and E)
- Never fly over people or moving vehicles
- Keep your drone in visual line of sight of pilot or visual observer
- Never fly near aircraft
- Never fly under the influence of drugs or alcohol
- Never fly near emergencies or public safety activities
- Register all drones in certain categories
- Operate during daylight hours only

It is important to note that the FAA does not operate Counter-sUAS systems itself, but rather pursues administrative remedies against the Special Security Instructions violators and does not engage the UAS in violation with immediate physical or electronic mitigation measures.[196] Where such security measures are necessary, the implementation is done by the federal departments with vested interest in the security of airspace. In addition to the civilian flight considerations addressed by the FAA, the Departments of Defense, Justice, and Homeland Security, among others, implement the national strategy to secure the airspace. The implementation of the national strategy on countering aviation threats is guided by the Aviation Operational Threat Response (AOTR) Plan,[197] setting out administrative responsibilities with the Department of Justice and the Department of Homeland Security, and Domestic Counter-UAS National Action Plan to close the authorities' shortfalls.

Within the DoD, the Secretary of the Army has been designated as the DoD Executive Agent for C-sUAS. The same directive (DoDD 3800.01E) established the Joint Counter-sUAS Office (JCO) to help identify and prioritize solutions, coordinate requirements, plan, program and budget for Research and Development across the military Services. DoD also developed a joint doctrinal approach to categorize the UAS aircraft into 5 groups, depending on their respective gross takeoff weight, operating altitude, and speed.[198] The DoD C-sUAS use policy relies on two primary sources of authority: 10 U.S.C. §130i and the Standing Rules for the Use of Force in CJCSI 3121.01B.

[195] 14 CFR § 107

[196] 14 C.F.R. § 99.7

[197] https://www.hsdl.org/c/view?docid=472111

[198] See Joint Air Operations, JP 3-30, Figure III-14;
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf

DoD enabling regulations and authorities:

10 U.S.C. § 130i shields against criminal liability and punitive measures for otherwise illegal activities in mitigating UAS threats. Protections only apply to the "covered assets and facilities," and only if a command is "130i-compliant." It provides for the use of means to:

- Detect, identify, monitor, and track ("DIMT")
- Warn sUAS operators
- Disrupt sUAS control
- Seize/exercise control over sUAS
- Seize/confiscate sUAS
- Use reasonable force to disable, damage, or destroy sUAS

Pursuant to the DoD Policy Memorandum 17-00X, the authority to execute C-sUAS measures under §130i has been assigned to the commanders of the "covered facilities and assets."[199] For the U.S. Army, the classified HQDA EXORD 149-23, "Army responsibilities and implementation instructions for C-sUAS," provides detailed federal inter-agency coordination instructions, procedures for conducting assessments and estimates, training and compliance requirements, spectrum coordination and samples of necessary reference forms.

Standing Rules for the Use of Force (SRUF) as defined under CJCSI 3121.01B, and as provided in the DepSecDef Policy Memorandum 16-003, "Interim Guidance for Countering Unmanned Aircraft," as supplemented by DepSecDef Policy Memorandum 17-00X, "Supplemental Guidance for Countering Unmanned Aircraft (UA)," provides authority to use C-sUAS measures in self-defense situations to mitigate physical threats that an UAS or UA poses to the safety and security of a covered facility or asset and the personnel taking part in activities involving a covered facility or asset. It also allows for protection of certain designated military property, such as Assets Vital to National Security or Inherently Dangerous Property, as defined by the SRUF. For the U.S. Army, the C-sUAS authorities and procedures have been further defined in the classified HQDA EXORD 149-23 for C-sUAS protection, and HQDA EXORD 268-23 for the UAS reporting requirements.

In addition to the DoD specific authorities described above, the C-sUAS operations in the Homeland could involve providing support to other governmental agencies under their specific authorities. It is important to have a basic awareness of these sources of authorities when considering operations during Defense Support of Civil Authorities (DSCA), especially as they relate to law enforcement, public security, transportation, or anti-terrorism. Some of these include:

Title 6 U.S.C. § 124n – Apply to the DHS and DoJ and enable protection of certain assets and facilities from credible threats to covered assets and facilities by unmanned

[199] DoD Policy Memorandum 17-00X, Supplemental Guidance for Countering Unmanned Aircraft (July 2017)

aircraft. Limited by the privacy and property rights, data retention of 180 days, mitigation requirements, congressional reporting requirements etc.

Title 50 U.S. Code § 2661 – Provide for the protection of certain nuclear facilities and assets from unmanned aircraft and enables the Department of Energy to execute some of the protection functions for their sensitive infrastructure.

Title 49 U.S.C. § 40103 – DoT through the FAA Administrator can establish areas in the airspace the Administrator decides are *necessary in the interest of national defense*; and by regulation or order, restrict or prohibit flight of civil aircraft that the Administrator cannot identify, locate, and control with available facilities in those areas.

Title 46 U.S. Code § 70051 - Regulation of anchorage and movement of vessels during national emergency. It provides for use of USCG (and potentially additional DoD assets) to protect ports from sabotage and disruption. Requires presidential declaration of national emergency.

UAS specific criminal law enforcement tools under Title 18 U. S. Code– Several criminal statutes can give rise to use of C-sUAS means and methods to prevent unlawful activities in the national airspace. These include:

- Knowing or reckless interference with manned aircraft (18 U.S.C. § 39B)
- Knowing operation in runway exclusion zone (18 U.S.C. § 39B)
- Knowing or reckless interference with wildfire suppression/emergency response (18 U.S.C. § 40A)
- Photographing certain defense installations (18 U.S.C. §§ 795 and 796) – use of aircraft for photographing and subsequent publication.[200]

Limitations of the C-sUAS activities:

When considering the legality of the C-sUAS measures to be implemented in the Homeland, it is imperative to consider the complex legal requirements defined in the federal law. Remember, UAS or UA activities of a nature of overflight or "surveillance" alone do not permit the use of force to damage, destroy, or disable such UAS or UA. Violating or exceeding the limited authority granted by 10 USC § 130i, SRUF, or other authorities for C-sUAS may violate numerous federal statutes, and potentially give rise to criminal and civil liabilities, depending on the nature and severity of the activity. It is important to be familiar with these limitations and incorporate them into the operational planning process:

a. The Fourth Amendment of the U.S. Constitution must be considered any time a search or a seizure of property occurs by the Government. In the case of C-sUAS activities, any time an sUAS is disabled, seized, or destroyed by a governmental entity, a "taking" or seizure under the Fourth Amendment occurs. The question becomes whether the seizure was lawful. Similarly, some

[200] Requires Presidential designation of covered military installations but does not impede overflight rights.

interception of communications signals between the operator and an sUAS may be considered a *search* of communications signals and is similarly protected under the Fourth Amendment.

b. The Destruction of Aircraft and Aircraft Facilities Act (also known as the Aircraft Sabotage Act) prohibits the damaging, destruction, disabling or wreckage of civil aircraft (which UAS technically are), or the causation of any aircraft to become unworkable, unusable, or hazardous to operate, or the conveyance of a threat to do so.[201]

c. Aircraft Piracy Statute prohibits seizing or exercising control of an aircraft in the special aircraft jurisdiction of the United States by force, violence, threat of force or violence, or any form of intimidation. Per statute, it specifically requires a wrongful intent on behalf of the entity seizing control of the aircraft.[202]

d. Wiretap Act prohibits acquisition of the *content* of communications without a warrant. It is a broad act and may include acquisition of video feeds or even sUAS control commands. Requires a careful consideration of the C-sUAS methods and distinction between passive detection and interception of communications.[203]

e. The Pen Register and Trap and Trace Statutes prohibit the installation's use of a pen register or trap and trace device without a court order.[204] The statutes further regulate the collection of routing, addressing, signaling and other non-content information for wire and electronic communications which deal with the signaling or routing commands, as well as the identification of information specific to the sUAS ID or ownership.

f. The Computer Fraud and Abuse Act prohibits illegal access to protected computers, as well as damage or use of those computers used for sUAS signaling or command routing.[205]

g. The Foreign Intelligence Surveillance Act (FISA) prohibits certain activities undertaken for foreign intelligence purposes unless specifically authorized by statute, and consistent with E.O. 12333, as amended by E.O. 13470.[206] FISA limitations also often involve questions of Intelligence Oversight and Sensitive Information rules in the legal analysis.

h. The "Anti-Jamming" Statutes prohibit willful or malicious interference with radio communications of licensed or authorized stations and systems.[207]

---

[201] 18 U.S.C. § 32

[202] 49 U.S.C. § 46502

[203] Title I of the Electronic Communications Privacy Act, referred to as the Wiretap Act, 18 USC §§ 2510-2523

[204] 18 U.S.C. §§ 3121-3127

[205] 18 U.S.C. § 1030

[206] 73 Fed. Reg. 43841, July 29, 2008

[207] 47 U.S.C. § 333, §§ 501-502

i. Signal Interference statutes criminalize willful or malicious interference in any way with the working or use of communication line, or system, or willful or malicious obstruction, hinderance, or delay of the transmission of any communication over any such line, or system (e.g. blocking telecommunication signals over an area).[208] Does not apply to lawful interference.

j. The Posse Comitatus Act [209]prohibits direct assistance to CLEAS, and specifically provides for punishment for violations under Title 18 of the U.S. Code by imprisonment of up to two (2) years, and/or fines. The considerations of legality under the Posse Comitatus Act in HD are a subject of a separate paragraph in this chapter and can involve complex analysis of the mobilization and operational authorities, as well as the type of activity, for the DoD force assisting the civilian agencies.

In addition to the statutory limitations described above, a thorough legal analysis of the C-sUAS plan must involve a consideration of the civil tort laws. While 10 U.S.C. §130i provides for liability immunity, actions under the SRUF or under other federal authorities might expose the military personnel to liability based on a proximate cause of damage. Targeting process must involve collateral damage estimates for both the effects on the violating aircraft, potential impact to the property on the ground, disruptions to other communications or air traffic, and the mitigation measures to minimize danger.

Therefore, the legal framework regulating the C-sUAS means and methods in the Homeland is complex and requires a very thorough and broad analysis. Effective C-sUAS planning must include a multi-layered approach, often including the measures in CYBER, electronic signals, space, navigable airspace. In just the last decade, addressing C-sUAS threats in the Homeland has become one of the fastest growing and most complex issues. The ubiquitous availability of cheap systems and ever-increasing technical capabilities of s-UAS require complex C-sUAS protection plans to properly account to the proliferation of lawful civilian UAS use, balanced against the interest in protecting certain facilities and activities.

R. Intelligence and information Gathering Activities during HD

In HD, DoD is the LFA charged with responsibility for the collection, analysis, retention, and dissemination of information and intelligence concerning the operational environment.[210] Depending on the type and nature of the HD operation, the intelligence

[208] 18 U.S.C. §§ 1362 & 1367

[209] as implemented under DODI 3025.21

[210] Intelligence Reform and Terrorism Prevention Act (IRTPA) formally reorganized the IC by amending the National Security Act of 1947 via the "National Security Intelligence Reform Act of 2004," which created the Office of the Director of National Intelligence. The IRTPA also revised the definition of "national intelligence" to clarify that the related constructs "national intelligence" and "intelligence related to the national security" refers to all intelligence, regardless of source, gathered within or outside the United States pertaining to more than one agency, and involving threats to U.S. people, property, or interests, the development or use of weapons of mass destruction (WMD), and any other matters bearing on U.S. national or homeland security. 50 U.S.C. §3003(5).

collection requirements can involve collection of any of the principal intelligence types: human, open source, signals, counterintelligence, geospatial, measurement and signature, and technical intelligence. In addition, the DoD intelligence personnel may be involved in collection of operational information, search and rescue, incidental gathering of criminal activity information, and other not-traditionally-intelligence activities. The type of activity, purpose of it, methods of collection, and dissemination requirements all impact the decision of what collection activities may be lawfully conducted in HD. Executive Order (E.O.) 12333, as amended, directs DoD elements of the Intelligence Community (IC) to disseminate all-source intelligence information (Defense Intelligence Agency (DIA)), signals intelligence information (National Security Agency (NSA)), and geospatial intelligence information (National Geospatial-Intelligence Agency (NGIA)) for foreign intelligence and counterintelligence purposes in support of national and departmental (i.e., defense) missions.[211] It also directs the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps to disseminate defense and defense-related intelligence and counterintelligence in support of departmental (i.e., defense) requirements, and national requirements (e.g., as in the case of terrorism information).

Contrast with other CCMDs: One of the most distinguishing features in HD is that the operational environment largely involves information on U.S. Persons (USP). The general rule is that the military intelligence assets will not engage in intelligence collection activities against USP unless the mission of the intelligence organization specifically permits collection on USP and the law authorizes the collection. This approach was borne out of existing constitutional and statutory protections of privacy and property rights in the U.S. DoD personnel are restricted from maintaining and collecting information about domestic activities of USP.[212] It is important not to assume that a CCDR has absolute plenary authority to execute intelligence gathering in an HD event. That authority remains subject to the Constitution, federal laws, Presidential Orders and SecDef direction and policy.[213] It is important to carefully review the purposes and methods for gathering required information, prior to engaging in collection.

Non-Privacy information requirements: Some HD operations may require information on matters such as State and local emergency management points of contact, emergency infrastructure information, terrain, weather conditions and patterns, weapons characteristics, and other types of collection efforts not directed against USP. Military intelligence assets may collect these types of information only IAW DOD 5240.1-R. Non-intelligence asset collection efforts shall be conducted IAW DODD 5200.27 as implemented by AR 380-13. Such information can include physical data relating to vital public or private installations, facilities, highways, and public utilities necessary to carry out an assigned DoD mission, e.g., reference or drop points on mapping systems,

---

[211] Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981) [hereafter E.O. 12333].

[212] *Id.*; DEP'T OF DEFENSE, DIR. 5240.01, DOD INTELLIGENCE ACTIVITIES (27 Aug. 2007) (Ch. 3, 9 Nov. 20); *see generally,* DEP'T OF THE ARMY, REG. 381-10, THE CONDUCT AND OVERSIGHT OF U.S. ARMY INTELLIGENCE ACTIVITIES (27 Jan. 2023).

[213] 10 U.S.C. § 164 (2023).

hospitals with specialized trauma capabilities, private locations with public staging areas that may be necessary for internally displaced persons movement.

Privacy and property rights protections: In contrast to gathering operational information, intelligence activities in HD will very often involve collection of USP and other protected information. The DoD activities are required to assure compliance with federal laws and regulations protecting personal rights and civil liberties in the homeland.[214] DoD Civil Liberties and Privacy Program, sets out the general compliance requirements.[215] The framework protecting the privacy rights is complex and involves: Constitutional protections, federal laws such as Privacy and Wiretap Act, DoD Directives and Instructions, service regulations, intelligence community directives (ICDs), National Security Council Intelligence Directives (NSCIDs), and Executive Orders among others.

Intelligence collection and oversight: The analysis and production by DoD intelligence assets of imagery and data collected during aerial reconnaissance in support of requests for assistance from a non-DoD entity for a "humanitarian" purpose is not a mission performed for intelligence collection purposes. The DoD intelligence actions consist of collection, production, analysis, and dissemination of defense related foreign intelligence and counterintelligence.[216] The Executive Order and DoD directives mandate that such intelligence activities be subjected to an intelligence oversight, designed to: protect USP constitutional rights and privacy, allow collection of authorized information by least intrusive means, and restrict dissemination for lawful government purposes only. DoD has implemented a structured intelligence oversight program, to monitor all levels of intelligence activities and assure compliance with the federal laws and regulations.[217]

Information collection: Requests for DoD intelligence asset aerial reconnaissance missions that are solely designed and intended to support civilian law enforcement agencies or for force protection purposes are not authorized, unless approved by the SecDef.[218] Force protection information support will be provided exclusively by the State and Federal law enforcement agencies, including DoD law enforcement authorities.

Any information collected during DoD intelligence asset aerial reconnaissance missions that relate to criminal activity or threats to DoD forces should be "incidental" collection and passed to Federal, State, and local law enforcement agencies IAW DOD 5240.1-R Procedure 12, and DODD 5505.17.[219] It may also be passed to military commanders for force protection purposes if the information collected indicates a direct threat to deployed DoD personnel, pursuant to DoDI 3025.21. In any of these cases, the operational information collection is subject to the Sensitive Information rules and

---

[214] *See,* DEP'T OF DEFENSE, INSTR. 52400.11, DOD PRIVACY AND CIVIL LIBERTIES PROGRAMS (29 Jan. 2019) (Ch. 1, 8 Dec. 20).
[215] *Id.*
[216] Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008).
[217] DEP'T OF DEFENSE, DIR. 5240.01, INTELLIGENCE OVERSIGHT (26 Apr. 2017).
[218] DODI 3025.21, *supra* note 96.
[219] DEP'T OF DEFENSE, INSTR. 5505.17, PERSONALLY IDENTIFIABLE INFORMATION AND LAW ENFORCEMENT INFORMATION HANDLING BY DOD LAW ENFORCEMENT ACTIVITIES (22 Aug. 2023).

regulations as they relate to publicly available information (PAI) gathering, privacy and civil liberties laws, and the directions promulgated by the President and SecDef.

Imagery or special collection taken during aerial reconnaissance for damage assessment, to determine lines of communications, navigable waterways and transportation routes shall not target USP. When aerial reconnaissance for the search and rescue (SAR) of a USP is conducted, implied consent for this type of collection may be reasonably assumed from a stranded person's personal desire to be located and rescued from imminent harm or danger.

Electronic Warfare vs SIGINT: Collecting information in the homeland electronic domain depends on the purpose for which the electronic signal information is being collected: whether for operational situational awareness, or as a part of SIGINT intelligence collection.[220] Examples of the former would be scans of electronic domain to detect incoming remotely controlled weapons, versus collecting intelligence on the type and properties of a signal to develop intelligence about the identity/origin of a controller. Technical authority to conduct Electronic Warfare operations rests with USSTRATCOM, with a USNORTHCOM Joint Electromagnetic Spectrum Operations (JEMSO) cell being responsible for the operations in this domain.[221] If the operations involve SIGINT, as described above, then coordination is required between USNORTHCOM and NSA, because it is the coordinator for all foreign signals intelligence gathering.[222]

CYBER domain collection: USCYBERCOM has the technical authority for execution of intelligence gathering operations in cyber domain.[223] Coordinating with USNORTHCOM and its subordinate commands, as well as other IC agencies, it provides situational awareness and access to regional or theater defensive cyber operations effects, enables intel gathering in cyber domain, and cyber support to operations.

Criminal information collection and dissemination: Information collected on USP by DOD personnel that indicates the existence of a threat to life or property, or the violation of law will be turned over to civilian law enforcement officials IAW DoDD 5200.27 and DoDD 5505.17, and will not be disseminated to DoD elements or retained in DoD files unless authorized by DOD 5240.1-R.

Receiving criminal and terrorism information: E.O. 13388 requires the head of any department/agency (including DoD and all Defense intelligence components) possessing or acquiring terrorism information, as defined in the IRTPA,[224] to share that information with other departments/agencies having counterterrorism responsibilities.

---

[220] DEP'T OF DEFENSE, INSTR. 3115.07, SIGNALS INTELLIGENCE (SIGINT) (15 Sep. 2008) (Ch. 2, 25 Aug. 20) [hereafter DODI 3115.07].

[221] *See generally,* JOINT CHIEFS OF STAFF, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTR. 3320.01 SERIES, JOINT ELECTROMAGNETIC SPECTRUM OPERATIONS.

[222] DODI 3115.07, *supra* note 218; PRESIDENTIAL POLICY DIRECTIVE-28, SIGNALS INTELLIGENCE ACTIVITIES (17 Jan 2014).

[223] DEP'T OF DEFENSE, INSTR. 8110.01, MISSION PARTNER ENVIRONMENT INFORMATION SHARING CAPABILITY IMPLEMENTATION FOR THE DOD (30 Jun. 21).

[224] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, sec. 1016(a)(4) (2004).

This includes all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:

> (1) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or other activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
>
> (2) threats posed by such groups or individuals to the U.S. or to other nations;
>
> (3) communications of or by such groups or individuals; or,
>
> (4) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.[225]

The criminal information and intelligence (CRIMINT) sharing regulatory framework also provides for a flow of information from the civilian law enforcement agencies back to the DoD under certain conditions. Federal law enforcement agencies and CRIMINT sharing systems are authorized sources of information in the information-gathering process. The information flow back to the DoD is proper where the civilian LEA identifies a force protection, counterintelligence, or foreign intelligence DoD nexus in the criminal information. DoD elements authorized to receive this information are those whose missions include responsibilities for counterintelligence, counternarcotics, personnel security, physical security and safety, DoD insider terrorist threats, foreign terrorist threats, and antiterrorism/force protection measures as defined by DoDI 5420.26, HRP as defined in DoDI O-2000.22, and DoDI 2000.12.

Conclusion: HD operations can involve the full spectrum of intelligence disciplines and intel collection in all domains. However, domestic laws protecting personal and civil rights, as well as coordinating requirements apply. Although the DoD is a lead federal agency for HD, it is still just one member of the Intelligence Community and must coordinate intel activities with interagency partners. E.O. 12333 assigns different agencies and agency heads as functional managers of certain intelligence disciplines. Any intelligence activities in these areas first require interagency coordination with the appropriate functional manager or their designee to conduct a proposed intel activity.

The JFLCC Inspector General, with collaboration by the ARNORTH Intelligence Attorney and G2 IO Officer, provides intelligence oversight.[226] Any mission that involves DoD intelligence components requires close coordination with the JFLCC and USNORTHCOM SJA to ensure intelligence oversight rules are followed. Questionable or illegal collection activities must be reported thru the chain of command to the Commander, JFLCC, ATTN: IG to the Department of the Army, ATTN: IG. The contents of the report to the Commander, JFLCC, will include the description of the incident; date, time, and place of the incident; summary; and status of the incident.

---

[225] *Id.*

[226] DEP'T OF DEFENSE, DIR. 5148.13, INTELLIGENCE OVERSIGHT (26 Apr. 2017) [hereafter DODD 5148.13].

S. "HD Activities" by the National Guard

Title 32 U.S.C. was amended in 2004 to give the SecDef the option to use National Guard forces for a "homeland defense activity" (HD activity) mission.[227] Specifically, the SecDef may, upon a request from a Governor, provide funds to employ National Guard Soldiers in a Title 32 status to conduct "HD activities."[228] Although very similar to the definition of HD, HD activity "means an activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States as determined by the Secretary of Defense to be critical to national security, from a threat or aggression against the United States." [229]

The main different between the definitions of HD and HD activity is that HD includes the protection of the "sovereignty of the U.S." and HD activity does not include this element. The responsibility for the protection of the sovereignty of the U.S. resides only with Title 10 forces under the control of the President and the SecDef.

The SecDef must also determine that the type of HD activity is "necessary and appropriate" for National Guard Soldiers to perform. In this regard, the Geographic CCDR shall advise the SecDef, through the Chairman of the Joint Chiefs of Staff, regarding the compatibility of the requested HD activity with ongoing HD operations.[230]

National Guard Soldiers performing HD activities remain under the command and control of the Governor. The duration of this duty is limited to 180 days but may be extended by the Governor with the concurrence of the SecDef for an additional 90 days to meet extraordinary circumstances. The State National Guard RUF applies under these circumstances instead of the SRUF.

T. Repatriation of U.S. Citizens

In a large-scale HD scenario, there would likely be many internal and external displaced persons who would require a system for relocation and settlement. The U.S. Repatriation Program potentially could become a model to follow to address a real and significant consideration for HD.

The U.S. Repatriation Program was established in 1935 under Section 1113 of the Social Security Act to provide "temporary assistance" to private U.S. citizens and their dependents identified by the Department of State (DOS) as having returned from a foreign country to the United States because of destitution, illness, war, threat of war, or a similar crisis, and are without available resources.[231]

---

[227] 32 U.S.C. §§ 901-908 (2023).

[228] DEP'T OF DEFENSE, DIR. 3160.01, HOMELAND DEFENSE ACTIVITIES CONDUCTED BY THE NATIONAL GUARD, para. 4a (25 Aug. 2008) (Ch. 2, 6 Jun. 2017).

[229] 32 U.S.C. § 901(1).

[230] *Id.* at Encl. 1, para. 8.

[231] 42 U.S.C. § 1313 (2023).

The 2021 National Emergency Repatriation Framework designated the Office of Human Services Emergency Preparedness and Response (OHSEPR) within the Administration for Children and Families (ACF) in the U.S. Department of Health and Human Services (HHS) as the domestic lead for the U.S. Repatriation Program. The Program is administered by the Office of Refugee Resettlement (ORR) within ACF. ORR partners with Department of State (DOS), state governments, and non-governmental organizations to aid repatriates.[232]

"Temporary assistance" is defined by Section 1113 of the Social Security Act as money payments, medical care, temporary billeting (e.g., public shelter), transportation, and other goods and services necessary for the health or welfare of individuals (including guidance, counseling, and other welfare services) provided to eligible repatriates within the United States.[233]

Every State has entered into a Standing Repatriation memorandum of agreement (MOA) with ACF/OHSEPR. IAW this MOA, the States that have a designated port of entry for repatriation (major international airports) are responsible for establishing the Emergency Repatriation Center (ERC) for the reception, temporary care, and onward transportation of eligible repatriates for up to 90 days. The States are the heavy lifters in this program.[234]

Collocated with the ERC is the DoD Joint Repatriation Processing Center (JRPC) established for the sole purpose of receiving and processing only DoD-affiliated members, such as DoD personnel and family members (does not include contractors) for onward movement to their final destination. The appropriate regional DCO/DCE will establish and collocate the JRPC with the ERC and immediate coordinate reach-back support from the nearest DoD installation/base that has the capacity to staff the JRPC with finance, medical, logistical, administrative, legal, etc. personnel and support. The DCO/DCE would execute this mission until transition with the arrival of the RFF units (approximately four days).[235]

U. Conclusion

The most important purpose and highest priority for the DoD is the defense of the homeland. Homeland defense is the military protection of U.S. sovereignty and territory against external threats and aggression or, as directed by the President, other threats. An external threat or aggression is an action, incident, or circumstance that originates from outside the boundaries of the homeland. However, threats planned to be executed by external actors may develop and/or take place inside the boundaries of the

---

[232] ADMINISTRATION FOR CHILDREN & FAMILIES, U.S. DEP'T OF HEALTH & HUMAN SERVICES, NATIONAL EMERGENCY REPATRIATION FRAMEWORK, pg. 4, (2010) [hereinafter NERF].

[233] 42 U.S.C. § 1313(c) (2023).

[234] NERF, *supra* note 229, at pg. 11.

[235] App 2 to Annex C to USARNORTH Supporting Plan to USNORTHCOM CONPLAN 3768-17, *Protection, Evacuation, Repatriation Operations in Response to Crises Abroad,* September 25, 2018.

homeland. DoD ensures the security of the United States by acting as a military deterrent to nations and groups who might otherwise wish to attack American soil and by pursuing and eliminating threats around the world. DoD combatant commands, military services, and defense agencies work to build the defense capacity of land HD taken under extraordinary circumstances to defeat land threats. Although the threat of a full-scale land invasion by a hostile power is remote, U.S. Army JAs must, nevertheless, take personal responsibility to prepare for and provide accurate and spontaneous advice and support to commanders conducting both offensive and defensive operations to withstand, respond to, and recover rapidly from strikes in a contested homeland environment.

ACRONYMS

AAMDC	**Army Air and Missile Defense Command**
ACF	**Administration for Children and Families**
AGR	**Active Guard Reserve**
AMD	**Air and Missile Defense**
AO	**Area of Operations**
AOR	**Area of Responsibility**
AOTR	**Aviation Operational Threat Response**
AR	**Army Regulation**
ARNORTH	**Army North**
ASCC	**Army Service Component Command**
ASD(HD&HA)	**Assistant Secretary of Defense (Homeland Defense and Hemispheric Affairs)**
ATTN	**Attention**
AVNS	**Asset Vital to National Security**
BCT	**Brigade Combat Team**
CAL	**Critical Assets List**
CBIRF	**Chemical Biological Incident Response Force**
CBRN	**Chemical, Biological, Radiological, and Nuclear**
CCDR	**Combatant Commander**
CERFP	**Chemical, Biological, Radiological, Nuclear and high-yield Enhanced Response Force Package**
CFR	**Code of Federal Regulations**
CIS	**Critical Infrastructure Sector**
CJCS	**Chairman Joint Chiefs of Staff**
CJCSI	**Chairman Joint Chiefs of Staff Instruction**
COCOM	**Combatant Command (a command authority)**

CONST	**Constitution**
CONUS	**Continental United States**
CRE	**CBRN Response Enterprise**
CRIMINT	**Criminal Intelligence**
CRPL	**CBRN Response Posture Level**
CRS	**Congressional Research Service**
C-sUAS	**Counter small Unmanned Aircraft System**
C2	**Command and Control**
C2CRE-A/B	**Command and Control CBRN Response Element – Alpha/Bravo**
DA	**Department of the Army**
DAJA-AL	**Department of the Army Judge Advocate – Administrative Law**
DAL	**Defended Assets List**
DCA	**Defense Critical Assets**
DCE	**Defense Coordinating Element**
DCI	**Defense Critical Infrastructure**
DCO	**Defense Coordinating Officer**
DCP	**Detainee Collection Point**
DCRF	**Defense CBRN Response Force**
DEPSECDEF	**Deputy Secretary of Defense**
DETOPS	**Detention Operations**
DHA	**Detainee Holding Area**
DHS	**Department of Homeland Security**
DIA	**Defense Intelligence Agency**
DIB	**Defense Industrial Base**
DIMT	**Detect, identify, monitor, and track**
DoD	**Department of Defense**
DODD	**Department of Defense Directive**
DODI	**Department of Defense Instruction**
DOJ	**Department of Justice**
DOS	**Department of State**
DRS	**Detainee Reporting System**
DSCA	**Defense Support of Civil Authority**
DVIDS	**Defense Visual Information Distribution Service**
EO	**Executive Order**
EPW	**Enemy Prisoner of War**
ERC	**Emergency Repatriation Center**
EXORD	**Execution Order**

FAA	**Federal Aviation Administration**
FEMA	**Federal Emergency Management Agency**
FM	**Field Manual**
FVEY	**FIVE EYES (Australia, Canada, New Zealand, United Kingdom and United States)**
FP	**Force Protection**
FORSCOM	**Forces Command**
GCC	**Geographical Combatant Command**
GFM	**Global Force Management**
GCIII	**Geneva Convention on Prisoners of War**
G2	**Military Intelligence staff position**
HD	**Homeland Defense**
HHS	**Health and Human Services**
HRF	**Homeland Response Force**
HRP	**High-Risk Personnel**
IAC	**International Armed Conflict**
IADS	**Integrated Air Defense System**
IAW	**In Accordance With**
IC	**Intelligence Community**
ICD	**Intelligence Community Directives**
ICRC	**International Committee of the Red Cross**
IDP	**Inherently Dangerous Property**
IG	**Inspector General**
IMA	**Individual Mobilization Augmentee**
IO	**Intelligence Oversight**
IRR	**Individual Ready Reserve**
IRTPA	**Intelligence Reform and Terrorism Prevention Act**
ISN	**Interment Serial Number**
JA	**Judge Advocate**
JCO	**Joint Counter-sUAS Office**
JEMSO	**Joint Electromagnetic Spectrum Operations**
JFLCC	**Joint Forces Land Component Commander**
JP	**Joint Publication**
JRPC	**Joint Repatriation Processing Center**
JTF-CS	**Joint Task Force Civil Support**
LEA	**Law Enforcement Agency**
LFA	**Lead Federal Agency**

LOAC	**Law of Armed Conflict**
METL	**Mission Essential Task List**
MI	**Military Intelligence**
MOA	**Memorandum of Agreement**
MOS	**Military Occupation Specialty**
MP	**Military Police**
NATO	**North Atlantic Treaty Organization**
NCI	**National Critical Infrastructure**
NCR	**National Capital Region**
NDAA	**National Defense Authorization Act**
NDAP	**Non-DoD Affiliated Person**
NED	**National Emergency Declaration**
NGA	**National Geospatial-Intelligence Agency**
NORAD	**North America Aerospace Defense Command**
NSA	**National Security Agency**
NSCID	**National Security Council Intelligence Directives**
OHSEPR	**Office of Human Services Emergency Preparedness and Response**
OPCON	**Operational Control**
ORR	**Office of Refugee Resettlement**
OTJAG	**Office of The Judge Advocate General**
PAI	**Publicly Available Information**
PCA	**Posse Comitatus Act**
POC	**Point of Capture**
PPD	**Presidential Policy Directive**
PRC	**People's Republic of China or President's Reserve Call-up**
PUB. L.	**Public Law**
QRF	**Quick Response Force**
RF	**Radio Frequency**
RFF	**Request for Forces**
RRF	**Rapid Response Force**
RUF	**Rules for the Use of Force**
SAR	**Search and Rescue**
SECDEF	**Secretary of Defense**

SIGINT	**Signals Intelligence**
SJA	**Staff Judge Advocate**
SLTT	**State, Local, Territorial, and Tribal**
SROE	**Standing Rules of Engagement**
SRUF	**Standing Rules for the Use of Force**
TCA	**Task Critical Asset**
TDF	**Theater Detention Facility**
TFR	**Temporary Flight Restriction**
TPU	**Troop Program Unit**
TQ	**Tactical Questioning**
UAS	**Unmanned Aircraft System**
UEB	**Unprivileged Enemy Belligerent**
US	**United States**
USACE	**United States Army Corps of Engineers**
USC	**United States Code**
USCG	**United States Coast Guard**
USCYBERCOM	**United States CYBER Command**
USGAO	**United States General Accounting Office**
USINDOPACOM	**United States Indo-Pacific Command**
USNORTHCOM	**United States Northern Command**
USP	**United States Persons**
USSTRATCOM	**United States Strategic Command**
WMD-CST	**Weapons of Mass Destruction Civil Support Team**
WW	**World War**