§ 394. Authorities concerning military cyber operations

(a) IN GENERAL.—The Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power.

(b) AFFIRMATION OF AUTHORITY.—Congress affirms that the activities or operations referred to in subsection (a), when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.)) or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States.

(c) CLANDESTINE ACTIVITIES OR OPERATIONS.—A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2)).

(d) CONGRESSIONAL OVERSIGHT.—The Secretary shall brief the congressional defense committees about any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, occurring during the previous quarter during the quarterly briefing required by section 484 of this title.

(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to authorize specific military activities or operations, or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or reporting of sensitive military cyber activities or operations required by section 395 of this title.

(f) DEFINITIONS.—In this section:

(1) The term ''clandestine military activity or operation in cyberspace'' means a military activity or military operation carried out in cyberspace, or associated preparatory actions, authorized by the President or the Secretary that—

(A) is marked by, held in, or conducted with secrecy, where the intent is that the activity or operation will not be apparent or acknowledged publicly; and

(B) is to be carried out—

(i) as part of a military operation plan approved by the President or the Secretary in anticipation of hostilities or as directed by the President or the Secretary;

(ii) to deter, safeguard, or defend against attacks or malicious cyber activities against the United States or Department of Defense information, networks, systems, installations, facilities, or other assets; or

(iii) in support of information related capabilities.

(2) The term ''foreign power'' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(3) The term ''United States person'' has the meaning given such term in such section.

(Added Pub. L. 114–92, div. A, title XVI, §1642(a), Nov. 25, 2015, 129 Stat. 1116, §130g; renumbered §394 and amended Pub. L. 115–232, div. A, title XVI, §§1631(a), 1632, Aug. 13, 2018, 132 Stat. 2123.)

REFERENCES IN TEXT

The War Powers Resolution, referred to in subsecs. (b) and (e), is Pub. L. 93–148, Nov. 7, 1973, 87 Stat. 555, which is classified generally to chapter 33 (§1541 et seq.) of Title 50, War and National Defense. For complete classification of this Resolution to the Code, see Short Title note set out under section 1541 of Title 50 and Tables.

The Authorization for Use of Military Force, referred to in subsec. (e), is Pub. L. 107–40, Sept. 18, 2001, 115 Stat. 224, which is set out as a note under section 1541 of Title 50, War and National Defense.

AMENDMENTS

2018—Pub. L. 115–232, §1632, designated existing provisions as subsec. (a), inserted heading, substituted ''conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response'' for ''conduct, a military cyber operation in response'', struck out ''(as such terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801))'' after ''foreign power'', and added subsecs. (b) to (f).

Pub. L. 115–232, §1631(a), renumbered section 130g of this title as this section.

POLICY OF THE UNITED STATES ON CYBERSPACE, CYBERSECURITY, CYBER WARFARE, AND CYBER DETERRENCE

Pub. L. 115–232, div. A, title XVI, §1636, Aug. 13, 2018, 132 Stat. 2126, provided that:

''(a) IN GENERAL.—It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests with the intent to—

''(1) cause casualties among United States persons or persons of United States allies;

''(2) significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government);

''(3) threaten the command and control of the Armed Forces, the freedom of maneuver of the Armed Forces, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or

''(4) achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States.

''(b) RESPONSE OPTIONS.—In carrying out the policy set forth in subsection (a), the United States shall plan, develop, and, when appropriate, demonstrate response options to address the full range of potential cyber at-

tacks on United States interests that could be conducted by potential adversaries of the United States.

''(c) DENIAL OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall, to the greatest extent practicable, prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities described in subsection (a) of infrastructure critical to the political integrity, economic security, and national security of the United States.

''(d) COST-IMPOSITION OPTIONS.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall develop and, when appropriate, demonstrate, or otherwise make known to adversaries the existence of, cyber capabilities to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity described in subsection (a).

''(e) MULTI-PRONG RESPONSE.—In carrying out the policy set forth in subsection (a) through response options developed pursuant to subsection (b), the United States shall leverage all instruments of national power.

''(f) UPDATE ON PRESIDENTIAL POLICY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the President shall transmit, in unclassified and classified forms, as appropriate, to the appropriate congressional committees a report containing an update to the report provided to the Congress on the policy of the United States on cyberspace, cybersecurity, and cyber warfare pursuant to section 1633 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 130g note) [now 10 U.S.C. 394 note].

''(2) CONTENTS.—The report required under paragraph (1) shall include the following:

''(A) An assessment of the current posture in cyberspace, including assessments of—

''(i) whether past responses to major cyber attacks have had the desired deterrent effect; and

''(ii) how adversaries have responded to past United States responses.

''(B) Updates on the Administration's efforts in the development of—

''(i) cost imposition strategies;

''(ii) varying levels of cyber incursion and steps taken to date to prepare for the imposition of the consequences referred to in clause (i); and

''(iii) the Cyber Deterrence Initiative.

''(C) Information relating to the Administration's plans, including specific planned actions, regulations, and legislative action required, for—

''(i) advancing technologies in attribution, inherently secure technology, and artificial intelligence society-wide;

''(ii) improving cybersecurity in and cooperation with the private sector;

''(iii) improving international cybersecurity cooperation; and

''(iv) implementing the policy referred to in paragraph (1), including any realignment of government or government responsibilities required, writ large.

''(f) [probably should be ''(g)''] RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to limit the authority of the President or Congress to authorize the use of military force.

''(g) [probably should be ''(h)''] DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(B) the Permanent Select Committee on Intelligence of the House of Representatives;

''(C) the Select Committee on Intelligence of the Senate;

''(D) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(E) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.

''(2) FOREIGN POWER.—The term 'foreign power' has the meaning given such term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).''

Pub. L. 115–91, div. A, title XVI, § 1633, Dec. 12, 2017, 131 Stat. 1738, provided that:

''(a) IN GENERAL.—The President shall—

''(1) develop a national policy for the United States relating to cyberspace, cybersecurity, and cyber warfare; and

''(2) submit to the appropriate congressional committees a report on the policy.

''(b) ELEMENTS.—The national policy required under subsection (a) shall include the following elements:

''(1) Delineation of the instruments of national power available to deter or respond to cyber attacks or other malicious cyber activities by a foreign power or actor that targets United States interests.

''(2) Available or planned response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(3) Available or planned denial options that prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

''(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

''(5) Development of multi-prong response options, such as—

''(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

''(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

''(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—

''(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

''(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

''(A) the White House Communication Agency; and

''(B) the White House Situation Support Staff.

''(d) DEFINITIONS.—In this section:

''(1) The term 'foreign power' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(2) The term 'appropriate congressional committees' means—

''(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.''

ACTIVE DEFENSE AGAINST THE RUSSIAN FEDERATION, PEOPLE'S REPUBLIC OF CHINA, DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA, AND ISLAMIC REPUBLIC OF IRAN ATTACKS IN CYBERSPACE

Pub. L. 115–232, div. A, title XVI, §1642, Aug. 13, 2018, 132 Stat. 2132, provided that:

''(a) AUTHORITY TO DISRUPT, DEFEAT, AND DETER CYBER ATTACKS.—

''(1) IN GENERAL.—In the event that the National Command Authority determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense to conduct cyber operations and information operations as traditional military activities.

''(2) NOTIFICATION AND REPORTING.—

''(A) NOTIFICATION OF OPERATIONS.—In exercising the authority provided in paragraph (1), the Secretary shall provide notices to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] in accordance with section 395 of title 10, United States Code (as transferred and redesignated pursuant to section 1631).

''(B) QUARTERLY REPORTS BY COMMANDER OF THE UNITED STATES CYBER COMMAND.—

''(i) IN GENERAL.—In any fiscal year in which the Commander of the United States Cyber Command carries out an action under paragraph (1), the Secretary of Defense shall, not less frequently than quarterly, submit to the congressional defense committees a report on the actions of the Commander under such paragraph in such fiscal year.

''(ii) MANNER OF REPORTING.—Reports submitted under clause (i) shall be submitted in a manner that is consistent with the recurring quarterly report required by section 484 of title 10, United States Code.

''(b) PRIVATE SECTOR COOPERATION.—The Secretary may make arrangements with private sector entities, on a voluntary basis, to share threat information related to malicious cyber actors, and any associated false online personas or compromised infrastructure, associated with a determination under subsection (a)(1), consistent with the protection of sources and methods and classification guidelines, as necessary.

''(c) ANNUAL REPORT.—Not less frequently than once each year, the Secretary shall submit to the congressional defense committees, the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), the Committee on Foreign Affairs of the House of Representatives, and the Committee on Foreign Relations of the Senate a report on—

''(1) the scope and intensity of the information operations and attacks through cyberspace by the countries specified in subsection (a)(1) against the government or people of the United States observed by the cyber mission forces of the United States Cyber Command and the National Security Agency; and

''(2) adjustments of the Department of Defense in the response directed or recommended by the Secretary with respect to such operations and attacks.

''(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

''(1) limit the authority of the Secretary to conduct military activities or operations in cyberspace, including clandestine activities or operations in cyberspace; or

''(2) affect the War Powers Resolution (Public Law 93–148; 50 U.S.C. 1541 et seq.) or the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note).''

PILOT PROGRAM TO MODEL CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Pub. L. 115–232, div. A, title XVI, §1649, Aug. 13, 2018, 132 Stat. 2137, provided that:

''(a) PILOT PROGRAM REQUIRED.—

''(1) IN GENERAL.—The Assistant Secretary of Defense for Homeland Defense and Global Security shall carry out a pilot program to model cyber attacks on critical infrastructure in order to identify and develop means of improving Department of Defense responses to requests for defense support to civil authorities for such attacks.

''(2) RESEARCH EXERCISES.—The pilot program shall source data from and include consideration of the 'Jack Voltaic' research exercises conducted by the Army Cyber Institute, industry partners of the Institute, and the cities of New York, New York, and Houston, Texas.

''(b) PURPOSE.—The purpose of the pilot program shall be to accomplish the following:

''(1) The development and demonstration of risk analysis methodologies, and the application of commercial simulation and modeling capabilities, based on artificial intelligence and hyperscale cloud computing technologies, as applicable—

''(A) to assess defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency;

''(B) to determine the likely effectiveness of attacks described in subsection (a)(1), and countermeasures, tactics, and tools supporting responsive military homeland defense operations;

''(C) to train personnel in incident response;

''(D) to conduct exercises and test scenarios;

''(E) to foster collaboration and learning between and among departments and agencies of the Federal Government, State and local governments, and private entities responsible for critical infrastructure; and

''(F) improve intra-agency and inter-agency coordination for consideration and approval of requests for defense support to civil authorities.

''(2) The development and demonstration of the foundations for establishing and maintaining a program of record for a shared high-fidelity, interactive, affordable, cloud-based modeling and simulation of critical infrastructure systems and incident response capabilities that can simulate complex cyber and physical attacks and disruptions on individual and multiple sectors on national, regional, State, and local scales.

''(c) REPORT.—

''(1) IN GENERAL.—At the same time the budget of the President for fiscal year 2021 is submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the Assistant Secretary shall, in consultation with the Secretary of Homeland Security, submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the pilot program.

''(2) CONTENTS.—The report required by paragraph (1) shall include the following:

''(A) A description of the results of the pilot program as of the date of the report.

''(B) A description of the risk analysis methodologies and modeling and simulation capabilities developed and demonstrated pursuant to the pilot program, and an assessment of the potential for future growth of commercial technology in support of the homeland defense mission of the Department of Defense.

''(C) Such recommendations as the Secretary considers appropriate regarding the establishment of a program of record for the Department on further development and sustainment of risk analysis methodologies and advanced, large-scale modeling and simulation on critical infrastructure and cyber warfare.

''(D) Lessons learned from the use of novel risk analysis methodologies and large-scale modeling and simulation carried out under the pilot program regarding vulnerabilities, required capabilities, and reconfigured force structure, coordination practices, and policy.

''(E) Planned steps for implementing the lessons described in subparagraph (D).

''(F) Any other matters the Secretary determines appropriate.''

IDENTIFICATION OF COUNTRIES OF CONCERN REGARDING CYBERSECURITY

Pub. L. 115–232, div. A, title XVI, § 1654, Aug. 13, 2018, 132 Stat. 2148, provided that:

''(a) IDENTIFICATION OF COUNTRIES OF CONCERN.—Not later than 180 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list. In creating such list, the Secretary shall take in to account the following:

''(1) A foreign government's activities that pose force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(2) A foreign government's willingness and record of providing financing, logistics, training or intelligence to other persons, countries or entities posing a force protection or cybersecurity risk to the personnel, financial systems, critical infrastructure, or information systems of the United States or coalition forces.

''(3) A foreign government's engagement in foreign intelligence activities against the United States for the purpose of undermining United States national security.

''(4) A foreign government's knowing participation in transnational organized crime or criminal activity.

''(5) A foreign government's cyber activities and operations to affect the supply chain of the United States Government.

''(6) A foreign government's use of cyber means to unlawfully or inappropriately obtain intellectual property from the United States Government or United States persons.

''(b) UPDATES.—The Secretary shall continuously update and maintain the list under subsection (a) to preempt obsolescence.

''(c) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the appropriate committees of Congress the list created pursuant to subsection (a) and any accompanying analysis that contributed to the creation of the list.''

§ 395. Notification requirements for sensitive military cyber operations

(a) IN GENERAL.—Except as provided in subsection (d), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation.

(b) PROCEDURES.—(1) The Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify the congressional defense committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a sensitive military cyber operation covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the sensitive military cyber operation concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) SENSITIVE MILITARY CYBER OPERATION DEFINED.—(1) In this section, the term ''sensitive military cyber operation'' means an action described in paragraph (2) that—

(A) is carried out by the armed forces of the United States; and

(B) is intended to cause cyber effects outside a geographic location—

(i) where the armed forces of the United States are involved in hostilities (as that term is used in section 1543 of title 50, United States Code); or

(ii) with respect to which hostilities have been declared by the United States.

(2) The actions described in this paragraph are the following:

(A) An offensive cyber operation.

(B) A defensive cyber operation outside the Department of Defense Information Networks to defeat an ongoing or imminent threat.

(d) EXCEPTIONS.—The notification requirement under subsection (a) does not apply—

(1) to a training exercise conducted with the consent of all nations where the intended effects of the exercise will occur; or

(2) to a covert action (as that term is defined in section 503 of the National Security Act of 1947 (50 U.S.C. 3093)).

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution (50 U.S.C. 1541 et seq.), the Authorization for Use of Military Force (Public Law 107–40; 50 U.S.C. 1541 note), or any requirement under the National Security Act of 1947 (50 U.S.C. 3001 et seq.).

(Added Pub. L. 115–91, div. A, title XVI, § 1631(a), Dec. 12, 2017, 131 Stat. 1736, § 130j; renumbered