prior to editorial reclassification and renumbering as section 3024 of this title.

CODIFICATION

Section was formerly classified as a note under section 403–1 of this title prior to editorial reclassification as this section.

§ 3367. Requirement for efficient use by intelligence community of open-source intelligence

The Director of National Intelligence shall ensure that the intelligence community makes efficient and effective use of open-source information and analysis.

(Pub. L. 108–458, title I, § 1052(b), Dec. 17, 2004, 118 Stat. 3683.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 403–1 of this title prior to editorial reclassification as this section.

§ 3368. Assistance for governmental entities and private entities in recognizing online violent extremist content

(a) Assistance to recognize online violent extremist content

Not later than 180 days after May 5, 2017, and consistent with the protection of intelligence sources and methods, the Director of National Intelligence shall publish on a publicly available Internet website a list of all logos, symbols, insignia, and other markings commonly associated with, or adopted by, an organization designated by the Secretary of State as a foreign terrorist organization under section 1189(a) of title 8.

(b) Updates

The Director shall update the list published under subsection (a) every 180 days or more frequently as needed.

(Pub. L. 115–31, div. N, title IV, § 403, May 5, 2017, 131 Stat. 820.)

§ 3369. Cooperative actions to detect and counter foreign influence operations

(a) Findings

Congress makes the following findings:

(1) The Russian Federation, through military intelligence units, also known as the ''GRU'', and Kremlin-linked troll organizations often referred to as the ''Internet Research Agency'', deploy information warfare operations against the United States, its allies and partners, with the goal of advancing the strategic interests of the Russian Federation.

(2) One line of effort deployed as part of these information warfare operations is the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion.

(3) These information warfare operations are a threat to the national security of the United States and that of the allies and partners of the United States. As former Director of National Intelligence Dan Coats stated, ''These actions are persistent, they are pervasive and they are meant to undermine America's democracy.''.

(4) These information warfare operations continue to evolve and increase in sophistication.

(5) Other foreign adversaries and hostile non-state actors are increasingly adopting similar tactics of deploying information warfare operations against the West, such as recent state-backed operations from China around the Hong Kong protests identified by social media companies.

(6) Technological advances, including artificial intelligence, will only make it more difficult in the future to detect fraudulent accounts, deceptive material posted on social media, and malign behavior on social media platforms.

(7) Because these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.

(8) The social media companies are inherently technologically sophisticated and adept at rapidly analyzing large amounts of data and developing software-based solutions to diverse and ever-changing challenges on their platforms, which makes them well-equipped to address the threat occurring on their platforms.

(9) Independent analyses confirmed Kremlin-linked threat networks, based on data provided by several social media companies to the Select Committee on Intelligence of the Senate, thereby demonstrating that it is possible to discern both broad patterns of cross-platform information warfare operations and specific fraudulent behavior on social media platforms.

(10) General Paul Nakasone, Director of the National Security Agency, emphasized the importance of these independent analyses to the planning and conducting of military cyber operations to frustrate Kremlin-linked information warfare operations against the 2018 midterm elections. General Nakasone stated that the reports ''were very, very helpful in terms of being able to understand exactly what our adversary was trying to do to build dissent within our nation.''.

(11) Institutionalizing ongoing robust, independent, and vigorous analysis of data related to foreign threat networks within and across social media platforms will help counter ongoing information warfare operations against the United States, its allies, and its partners.

(12) Archiving and disclosing to the public the results of these analyses by the social media companies and trusted third-party experts in a transparent manner will serve to demonstrate that the social media companies are detecting and removing foreign malign activities from their platforms while protecting the privacy of the people of the United States and will build public understanding of the

scale and scope of these foreign threats to our democracy, since exposure is one of the most effective means to build resilience.

(b) Sense of Congress

It is the sense of Congress that—

(1) the social media companies should cooperate among themselves and with independent organizations and researchers on a sustained and regular basis to share and analyze data and indicators relevant to foreign information warfare operations within and across their platforms in order to detect and counter foreign information warfare operations that threaten the national security of the United States and its allies and partners;

(2) information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations;

(3) these analytic efforts should be organized in such a fashion as to meet the highest standards of ethics, confidentiality, and privacy protection of the people of the United States, while still allowing timely research access to relevant data;

(4) these analytic efforts should be undertaken as soon as possible to facilitate countering ongoing state or state-backed foreign information warfare operations and to aid in preparations for the United States Presidential and congressional elections in 2020 and beyond;

(5) the structure and operations of social media companies make them well positioned to work with independent organizations and researchers to address foreign adversary threat networks within and across their platforms, and these efforts could be conducted without direct Government involvement, direction, or regulation; and

(6) if the social media industry fails to take sufficient action to address foreign adversary threat networks operating within or across their platforms, Congress would have to consider additional safeguards for ensuring that this threat is effectively mitigated.

(c) Requirement to facilitate establishment of Social Media Data and Threat Analysis Center

(1) Requirement

Not later than June 1, 2021, the Director of National Intelligence, in coordination with the Secretary of Defense, shall facilitate, by grant or contract or under an existing authority of the Director, the establishment of a Social Media Data and Threat Analysis Center with the functions described in paragraph (2) at an independent, nonprofit organization.

(2) Functions

The functions described in this paragraph are the following:

(A) Acting as a convening and sponsoring authority for cooperative social media data analysis of foreign threat networks involving social media companies and third-party experts, nongovernmental organizations, data journalists, Federally funded research and development centers, academic researchers, traditional media, and international counterparts, as appropriate.

(B) Facilitating analysis of foreign influence operation, within and across the individual social media platforms as well as hacking and leaking campaigns, and other tactics, and related unlawful activities that fund or subsidize such operations.

(C) Developing processes to share information from government entities on foreign influence operations with the individual social media companies to inform threat analysis, and working with the Office of the Director of National Intelligence as appropriate.

(D) Determining and making public criteria for identifying which companies, organizations, or researchers qualify for inclusion in the activities of the Center, and inviting entities that fit the criteria to join.

(E) Determining jointly with the social media companies what data and metadata related to indicators of foreign adversary threat networks from their platforms and business operations will be made available for access and analysis.

(F) Developing and making public the criteria and standards that must be met for companies, other organizations, and individual researchers to access and analyze data relating to foreign adversary threat networks within and across social media platforms and publish or otherwise use the results.

(G) Developing and making public the ethical standards for investigation of foreign threat networks and use of analytic results and for protection of the privacy of the customers and users of the social media platforms and of the proprietary information of the social media companies.

(H) Developing technical, contractual, and procedural controls to prevent misuse of data, including any necessary auditing procedures, compliance checks, and review mechanisms.

(I) Developing and making public criteria and conditions under which the Center shall share information with the appropriate Government agencies regarding threats to national security from, or violations of the law involving, foreign activities on social media platforms.

(J) Hosting a searchable archive aggregating information related to foreign influence and disinformation operations to build a collective understanding of the threats and facilitate future examination consistent with privacy protections.

(K) Developing data standards to harmonize the sharing of information pursuant to this paragraph.

(d) Reporting and notifications

The Director of the Center shall—

(1) not later than August 1, 2021, submit to appropriate congressional committees a report on—

(A) the estimated funding needs of the Center for fiscal year 2021 and for subsequent years;

(B) such statutory protections from liability as the Director considers necessary for the Center, participating social media com-

panies, and participating third-party analytical participants;

(C) such statutory penalties as the Director considers necessary to ensure against misuse of data by researchers; and

(D) such changes to the Center's mission to fully capture broader unlawful activities that intersect with, complement, or support information warfare tactics; and

(2) not less frequently than once each year, submit to the Director of National Intelligence, the Secretary of Defense, and the appropriate congressional committees a report—

(A) that assesses—

(i) degree of cooperation and commitment from the social media companies to the mission of the Center; and

(ii) effectiveness of the Center in detecting and facilitating the removal or neutralization of clandestine foreign information warfare operations from social media platforms; and

(B) includes such recommendations for legislative or administrative action as the Center considers appropriate to carry out the functions of the Center.

(e) Periodic reporting to the public

The Director of the Center shall—

(1) once each quarter, make available to the public a report on key trends in foreign influence and disinformation operations, including any threats to campaigns and elections, to inform the public of the United States; and

(2) as the Director considers necessary, provide more timely assessments relating to ongoing disinformation campaigns.

(f) Foreign malign influence campaigns on social media platforms targeting elections for Federal office

(1) Reports

(A) Requirement

Not later than 90 days before the date of each regularly scheduled general election for Federal office, the Director of the Center shall submit to the appropriate congressional committees a report on foreign malign influence campaigns on and across social media platforms targeting such election.

(B) Matters included

Each report under subparagraph (A) shall include an analysis of the following:

(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

(ii) Inauthentic accounts and ''bot'' networks across platforms, including the scale to which such accounts or networks exist, how platforms currently act to remove such accounts or networks, and what percentage of such accounts or networks have been removed during the period covered by the report.

(iii) The estimated reach and impact of intentional or weaponized disinformation by inauthentic accounts and ''bot'' networks, including an analysis of amplification by users and algorithmic distribution.

(iv) The trends of types of media that are being used for dissemination through foreign malign influence campaigns, including machine-manipulated media, and the intended targeted groups.

(C) Initial report

Not later than August 1, 2021, the Director of the Center shall submit to the appropriate congressional committees a report under subparagraph (A) addressing the regularly scheduled general election for Federal office occurring during 2020.

(D) Form

Each report under this paragraph shall be submitted in an unclassified form, but may include a classified annex.

(2) Briefings

(A) Requirement

Not later than 30 days after the date on which the Director submits to the appropriate congressional committees a report under paragraph (1), the Director of National Intelligence, in coordination with the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, shall provide to such committees a briefing assessing threats from foreign malign influence campaigns on social media from covered countries to the regularly scheduled general election for Federal office covered by the report.

(B) Matters to be included

Each briefing under subparagraph (A) shall include the following:

(i) The patterns, tools, and techniques of foreign malign influence campaigns across all platforms on social media by a covered foreign country targeting a regularly scheduled general election for Federal office.

(ii) An assessment of the findings from the report for which the briefing is provided.

(iii) The activities and methods used to mitigate the threats associated with such findings by the Department of Defense, the Department of Homeland Security, or other relevant departments or agencies of the Federal Government.

(iv) The steps taken by departments or agencies of the Federal Government to cooperate with social media companies to mitigate the threats identified.

(g) Funding

Of the amounts appropriated or otherwise made available to the National Intelligence Program (as defined in section 3003 of this title) in fiscal year 2021 and 2022, the Director of National Intelligence may use up to $30,000,000 to carry out this section.

(h) Definitions

(1) Appropriate congressional committees

The term ''appropriate congressional committees'' means—

(A) the congressional intelligence committees;

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

(C) the Committee on Armed Services, the Committee on Appropriations, the Committee on Homeland Security and Government Affairs, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate.

(2) Covered foreign country and foreign malign influence

The terms ''covered foreign country'' and ''foreign malign influence'' have the meanings given those terms in section 3059 of this title.

(3) Machine-manipulated media

The term ''machine-manipulated media'' has the meaning given that term in section 5724.

(Pub. L. 116–92, div. E, title LIII, § 5323, Dec. 20, 2019, 133 Stat. 2130; Pub. L. 116–283, div. H, title XCIII, § 9301, Jan. 1, 2021, 134 Stat. 4801.)

Editorial Notes

REFERENCES IN TEXT

Section 5724, referred to in subsec. (h)(3), is section 5724 of Pub. L. 116–92, which is set out as a note under section 3024 of this title.

AMENDMENTS

2021—Pub. L. 116–283, § 9301(d)(3)(A), struck out ''Encouragement of'' before ''Cooperative'' in section catchline.

Subsec. (c). Pub. L. 116–283, 9301(d)(3)(B)(i), substituted ''Requirement'' for ''Authority'' in heading.

Subsec. (c)(1). Pub. L. 116–283, § 9301(a), (d)(3)(B)(ii), in heading, substituted ''Requirement'' for ''Authority'' and, in text, substituted ''Not later than June 1, 2021, the Director'' for ''The Director'' and ''shall'' for ''may''.

Subsec. (d). Pub. L. 116–283, § 9301(d)(1)(A), substituted ''The'' for ''If the Director of National Intelligence chooses to use funds under subsection (c)(1) to facilitate the establishment of the Center, the'' in introductory provisions.

Subsec. (d)(1). Pub. L. 116–283, § 9301(d)(1)(B), substituted ''August 1, 2021'' for ''180 days after December 20, 2019''.

Subsec. (f). Pub. L. 116–283, § 9301(b)(2), added subsec. (f). Former subsec. (f) redesignated (g).

Subsec. (g). Pub. L. 116–283, § 9301(d)(2), substituted ''fiscal year 2021 and 2022'' for ''fiscal year 2020 and 2021''.

Pub. L. 116–283, § 9301(b)(1), redesignated subsec. (f) as (g). Former subsec. (g) redesignated (h).

Subsec. (h). Pub. L. 116–283, § 9301(c), amended subsec. (h) generally. Prior to amendment, subsec. (h) defined ''appropriate congressional committees''.

Pub. L. 116–283, § 9301(b)(1), redesignated subsec. (g) as (h).

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of ''intelligence community'', referred to subsec. (b)(2), see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3369a. Report on deepfake technology, foreign weaponization of deepfakes, and related notifications

(a) Report on foreign weaponization of deepfakes and deepfake technology

(1) Report required

Not later than 180 days after December 20, 2019, the Director of National Intelligence, in consultation with the heads of the elements of the intelligence community determined appropriate by the Director, shall submit to the congressional intelligence committees a report on—

(A) the potential national security impacts of machine-manipulated media (commonly known as ''deepfakes''); and

(B) the actual or potential use of machine-manipulated media by foreign governments to spread disinformation or engage in other malign activities.

(2) Matters to be included

The report under subsection (a) shall include the following:

(A) An assessment of the technical capabilities of foreign governments, including foreign intelligence services, foreign government-affiliated entities, and foreign individuals, with respect to machine-manipulated media, machine-generated text, generative adversarial networks, and related machine-learning technologies, including—

(i) an assessment of the technical capabilities of the People's Republic of China and the Russian Federation with respect to the production and detection of machine-manipulated media; and

(ii) an annex describing those governmental elements within China and Russia known to have supported or facilitated machine-manipulated media research, development, or dissemination, as well as any civil-military fusion, private-sector, academic, or nongovernmental entities which have meaningfully participated in such activities.

(B) An updated assessment of how foreign governments, including foreign intelligence services, foreign government-affiliated entities, and foreign individuals, could use or are using machine-manipulated media and machine-generated text to harm the national security interests of the United States, including an assessment of the historic, current, or potential future efforts of China and Russia to use machine-manipulated media, including with respect to—

(i) the overseas or domestic dissemination of misinformation;

(ii) the attempted discrediting of political opponents or disfavored populations; and

(iii) intelligence or influence operations directed against the United States, allies or partners of the United States, or other jurisdictions believed to be subject to Chinese or Russian interference.

(C) An updated identification of the countertechnologies that have been or could