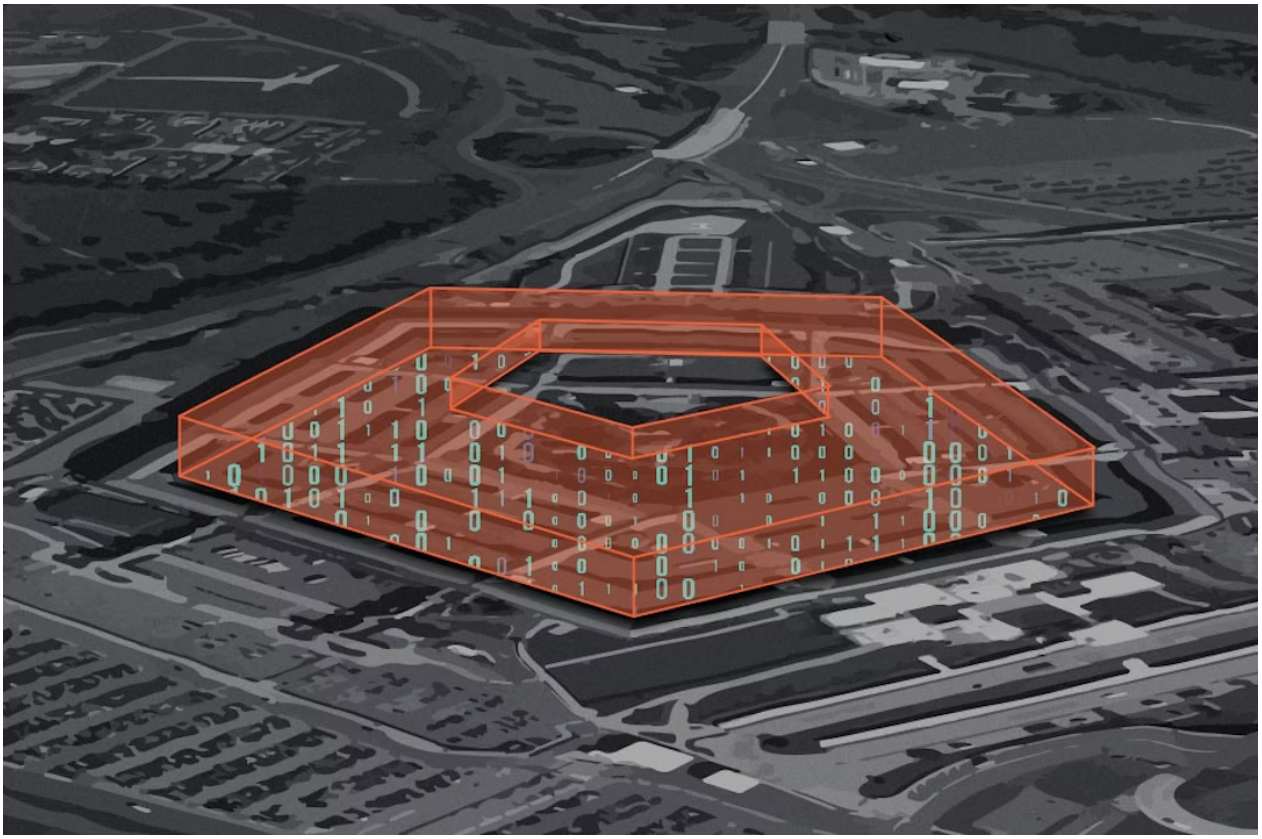
THIRD WAY

MEMO *Published April 5, 2021 • 19 minute read*

The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act



Michael Garcia
Former Senior Policy Advisor
@garrrcya

Takeaways

With Congress struggling to pass stand-alone cybersecurity legislation, the National Defense Authorization Act (NDAA) is now the primary vehicle to pass all matters of cybersecurity legislation. Because the annual defense bill typically requires provisions to have a tie to national security, other cyber issues, like those pertaining to criminal justice, tend to be excluded. As a result, the authorities and resources awarded to Department of Defense (DoD) cyber mission far outpace those provided to civilian agencies responsible for partnering with state, local, private, and international partners. With ransomware and cyber incidents at an all-time high, Congress should either include a new title in future Defense bills to bolster US

cyber enforcement and civilian agencies' capabilities or pass a cyber-omnibus bill to fix policy gaps and provide commensurate funds to federal and local agencies to combat malicious cyber activity.

In this paper, we analyzed the last five NDAAs (2017-2021) to chronicle Washington's reliance on the NDAA to shepherd through a wide swath of cybersecurity legislation. We found that:

- Members of Congress included 290 cyber-related provisions in the past five NDAAs, with the past two NDAAs accounting for 60% of those provisions. In fact, the FY 2021 NDAA contained 380% more cyber-related provisions than the FY 2017 NDAA.
- The 179 cyber-provisions included in the past two NDAAs far outpace the 14 cybersecurity bills that the 116 th Congress passed (two of which were those NDAAs).
- Across 13 categories, three of the top four were aimed at the DOD core cyber missions, such as changing organizational processes and structures, protecting DoD assets, and engaging with foreign partners while deterring nation-state adversaries.
- In FY 2020, the number of non-DoD-related cyber provisions began increasing, such as supply-chain security and industrial policy, critical infrastructure protection, and election security.

The provisions in these NDAAs helped improve US offensive cyber capabilities, implement measures to deter cyber adversaries, and shore up our cybersecurity defenses, all of which are needed. But because cybersecurity is a multifaceted issue that expands beyond national security and touches on criminal justice, workforce development, private-sector collaboration, and privacy issues, Congress must ensure it takes a holistic approach when creating cybersecurity laws.

The United States is facing a cyber epidemic.

Malicious cyber actors are attacking every facet of US society, causing high financial and societal costs. Within his first few days of office, Homeland Security Secretary Alejandro Mayorkas stated that the US government is currently fighting an epidemic in cyberspace wrought by ransomware. [1] Ransomware increased over 150% in 2020 compared to 2019, [2] impacting at least 80 hospitals [3] and a host of K-12 educational institutions. [4] Cybercriminals are the primary perpetrators of these crimes, who were responsible for 86% of all cyber incidents in 2020, up from 71% in 2019. [5] The costs of these incidents are alarming. According to McAfee, a cybersecurity firm, the cost of global cybercrime between 2018-2020 was over $1 trillion. [6] More worrisome than the economic impact of these incidents are the physical ramifications. In Florida, a hacker infiltrated a water treatment

plant's industrial control system and changed the levels of a chemical known as lye to lethal levels but was caught before it could impact the water. [7]

The US government has taken a whole-of-society approach to respond to these events and impose consequences on the perpetrators. Most notably, the Federal Bureau of Investigations (FBI), Europol, and private-sector companies collaborated to take down servers and arrest criminals behind one of the most notorious malware in the world, EMOTET. [8] At the state level, governors have deployed National Guard units to assist schools and election administrators in recovering from ransomware attacks and protecting against malicious cyber activities. [9] And if it were not for the cybersecurity firm FireEye's voluntary reporting that they were breached, the US government and Fortune 500 Companies may have never found out about the largest cyber-espionage incident in US history, the SunBurst hack (aka SolarWinds Hack).

These actions should be applauded, but Congress understands that it must institutionalize these relationships and provide partners additional resources to prepare for, respond to, investigate, and recover from cyber incidents.

Congress has increasingly introduced cyber-related legislation to address the cyber threat, but most Congressional action on cybersecurity occurs in the annual National Defense Authorization Act.

Members of Congress have increasingly grown comfortable tackling complicated cybersecurity issues, with the 116 th Congress introducing 40% more cyber-related bills than the previous session. [10] In fact, the 116 th and 115 th congressional sessions combined introduced 542 cyber-related bills, with a majority having bipartisan sponsorship. Yet, of those bills, only 24 became law. [11]

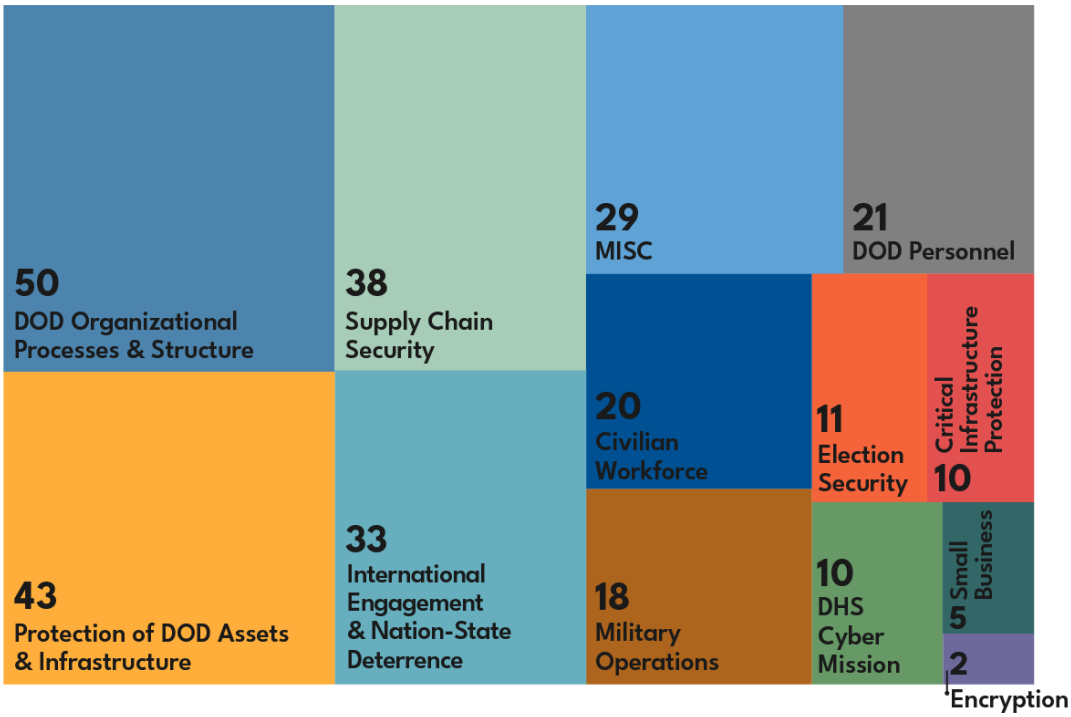
Congress did use some of the bills that passed both chambers as legislative vehicles to either attach previously introduced cyber bills or create entirely new cyber provisions. In terms of the former, the 116 th Congress included at least 45 cyber-related bills to appropriations and authorizations legislation, with 32 of those bills incorporated into the FY 2020 and FY 2021 NDAAs. [12] Some of these provisions have significant outcomes, such as creating the National Cyber Director, which is a senate-confirmed position that acts as the president's senior cyber advisor. [13] However, this only tells a fraction of the story, as Members of Congress have included hundreds of cyber provisions in the past five NDAAs that were never previously introduced.

Congress created 290 cyber-related provisions in the past five NDAAs (FY 2017-FY 2021), covering a range of 13 categories that predominantly focus on DoD's cyber mission. The majority of these provisions modified DoD's organizational processes and structure; protected DoD assets; and required DoD to engage with foreign partners and deter malicious nation-state actors (see

"Number of Sections per Category from FY 2017-FY 2021 NDAAs" graph). As discussed below, some of these provisions may (1) impact states' abilities to respond to cybercrime and other incidents, (2) be replicated in other civilian agencies, and (3) shape our international cybercrime strategy.

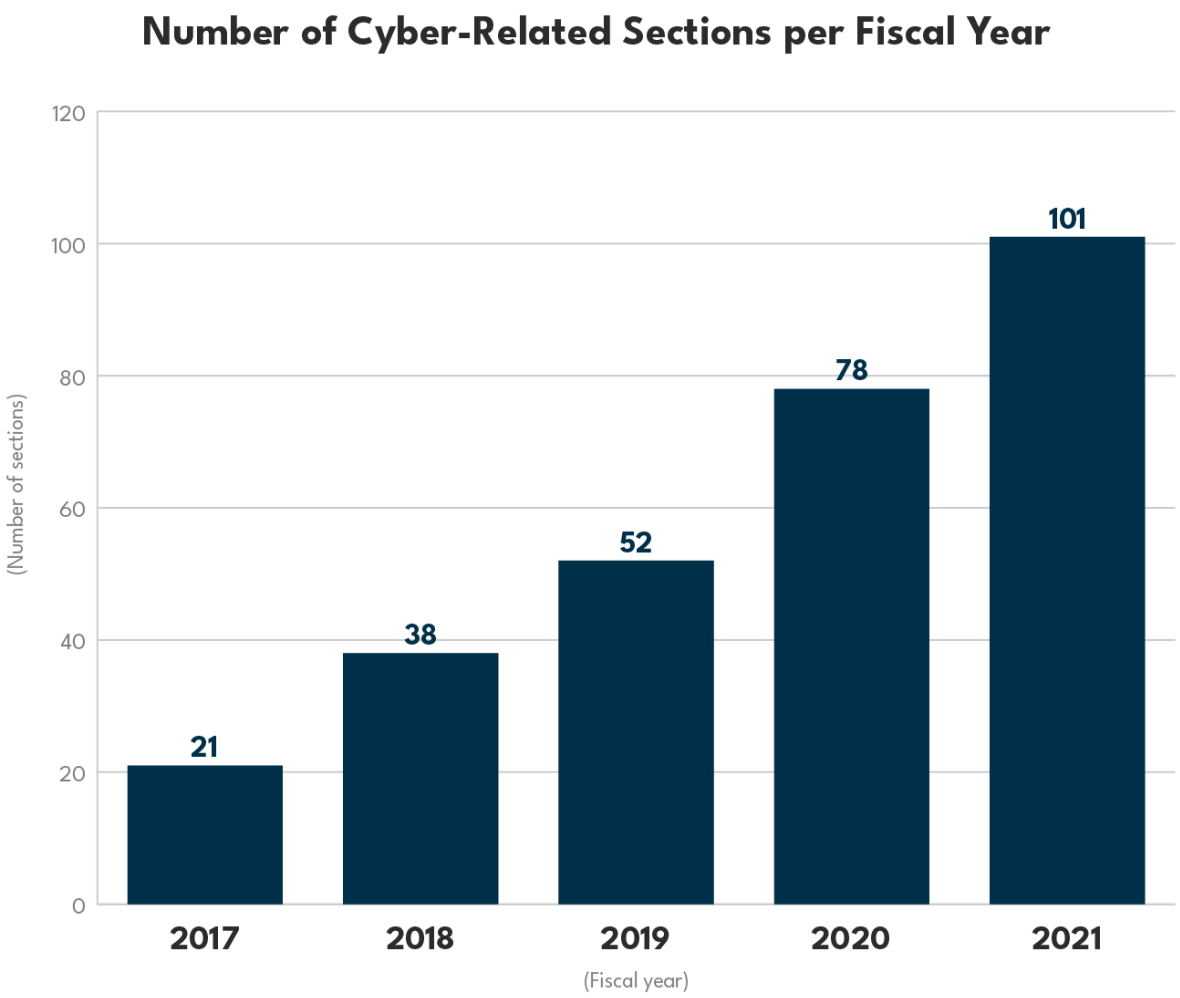
THIRD WAY

Number of Sections per Category From FY 2017-2021 NDAAs



Source: Based on Third Way research.

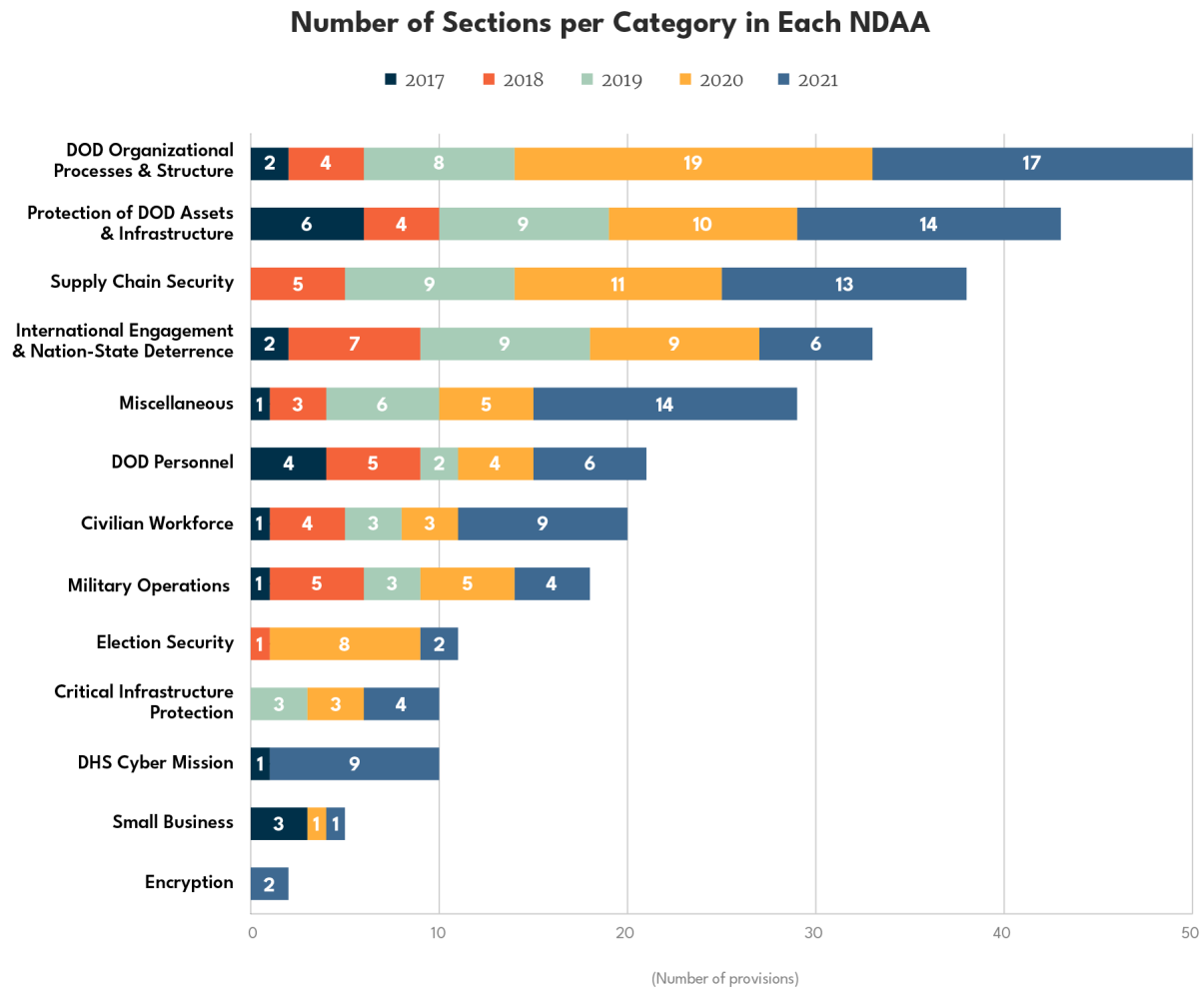
The FY 2020 and FY 2021 NDAAs accounted for 60% of all cyber provisions, with the FY 2021 NDAA containing 380% more cyber-related provisions than the FY 2017 NDAA (see "Number of Cyber-Related Sections per Fiscal Year" graph).



Source: Based on Third Way research.

The reason for this increase is two-fold. First, beginning in FY 2020, the number of non-DOD-related cyber provisions began increasing, such as measures directed at election security, critical infrastructure security (excluding the defense industrial base), and supply-chain security (See "Number of Sections per Category in Each NDAA" graph). Second, the US Cyberspace Solarium Commission (CSC)—a congressionally mandated commission that developed recommendations to improve US-cyber deterrence—created recommendations that accounted for 26% of all the cyber-related provisions in the FY 2021 NDAA.[14] As a result, the 179 cyber-provisions included in the past two NDAAs far outpace the 14 cybersecurity bills that the 116th Congress passed (two of which were those NDAAs).

While the non-DoD cyber provisions—Civilian Workforce, Election Security, Department of Homeland Security (DHS) Cyber Mission, Critical Infrastructure Protection, Small Business, Encryption, and provisions within supply-chain security and miscellaneous categories—are small in number, they have significant policy implications.



Source: Based on Third Way research.

Three of the top four categories were aimed at DoD's core cyber missions, such as modifying its organizational processes and structure; protecting DoD assets; and requiring DoD to engage with foreign partners while deterring nation-state adversaries.

DoD Organizational Processes and Structure

Most provisions dealt with DoD's organizational processes and structures, which created various cybersecurity positions within DoD's chain of command, assessments of cyber capabilities, budget authorities, and new authorizations or reporting requirements for cyber-related missions. Notably, these provisions established a unified combatant command for cyber operations within DoD, [15] required two cyber posture reviews to assess DoD's capabilities to perform cyber operations, [16] and

established a series of requirements if Cyber Command ever separates from the National Security Agency (known as the dual-hat arrangement). [17]

Several provisions also modified the National Guard's cyber capabilities, potentially impacting how governors could respond to cybercrimes (like ransomware) and other incidents. For example, the FY 2018 NDAA authorized the Secretary of Defense to conduct cyber threat exercises on election systems and report to Congress how the National Guard could assist states in defending those systems against cyberattacks. [18] Two provisions in the FY 2021 NDAA may also expand the National Guard's cyber responsibilities. The first is a pilot program to determine how National Guard units could provide remote assistance to other units to help states train, prepare for, and respond to cyber incidents. [19] The second will detail when a governor could deploy their National Guard units to respond to cyber incidents with federal reimbursement (known as Title 32 operations) and prescribe how the National Guard would collaborate with other civilian agencies to respond to a cyberattack. [20]

Limiting or expanding the Guard's cybersecurity authorities is within the Secretary of Defense's purview. Yet, with limited federal grants available to states and locals to improve their civilian protection and response efforts, [21] these limitations or expansions will greatly affect how states and locals can cope with cyber incidents. Policymakers must be aware of the outcome of these provisions and shore up civilian assets to complement the Guard's activities while incorporating the Guard's capabilities in incident-response plans. However, outside of a few provisions that empowered DHS to help states and locals and provided election-security assistance, the NDAAs did little to help states and locals.

Protection of DoD Assets and Infrastructure

The second-largest category included provisions that required DoD to protect weapon systems, the defense industrial base, and DoD's information network (DoDIN). [22] Although these provisions do not directly impact cyber issues outside of DoD's realm, they could one day be mirrored in civilian agencies who interact with the larger private-sector enterprise. For instance, the FY 2021 NDAA requires DoD contractors and subcontractors to report when their networks have been penetrated. [23] How DoD implements this program and lessons learned may influence current Congressional debates on developing a data breach and incident notification law. Another example is a framework that DoD must develop to enhance the cybersecurity of the DIB, which would establish and ensure compliance with cybersecurity standards, regulations, and policies. [24] While DoD has an unparalleled and unique relationship with defense contractors compared to other federal agencies' partnerships with companies, lessons learned from these programs may guide Congressional action as they consider implementing similar measures across civilian agencies.

International Engagement and Nation-State Deterrence

The third-largest DoD-related category (fourth-largest overall) was provisions that fostered engagement with international partners to improve their cybersecurity posture, as well as policies to deter nation-state actors from conducting cyberattacks. Like other operational domains, DoD has an imperative to collaborate with allies in cyberspace. Since 2017, Congress has tasked DoD to strengthen the North Atlantic Treaty Organization's cyber defenses, [25] work with Baltic countries to improve their cybersecurity posture, [26] and consider engaging in cyber exercises with allies in the Indo-Pacific. [27] The last five NDAAs also emphasize the need to deter nation-state adversaries in cyberspace—specifically China, Russia, Iran, and North Korea—with Congress mandating reports on how DoD deters these actors in FY 2017, 2018, and 2019. [28]

As a part of the US cyber-deterrent strategy, Congress included several measures that impose consequences on bad actors and hold them to account for their malicious cyber activities, like cybercrime. For example, the FY 2020 and FY 2021 NDAAs require DoD to assess North Korea's revenue generated from their cybercrime activities and provide recommendations on how to counter China's industrial espionage and intellectual-property theft. [29] Similarly, an FY 2019 provision requires the Secretary of Defense to create a list of countries that pose a risk to US cybersecurity, including those that knowingly participate in criminal activity. [30] Lastly, the FY 2021 NDAA establishes a Joint Cyber Planning Office within DHS, allowing federal agencies to collaborate with private entities to develop plans that disrupt the cyber infrastructure that cybercriminals use to conduct malicious cyber activities, like ransomware attacks. [31]

While these measures could deter cybercriminals and the nation-states that abet them, they do not impact other cyber enforcement areas. For instance, state and local law enforcement agencies require more resources to bolster their digital forensic capabilities to identify cybercriminals. [32] The State Department, too, requires additional authorities and resources to support international partners' efforts to improve their cybercrime enforcement capacity. As a result, the tools and resources available to the US government and its partners to pursue cybercriminals remain limited.

Beginning in FY 2020, the number of non-DoD-related cyber provisions began increasing, such as supply-chain security and industrial policy; critical infrastructure protection; and election security.

Supply-Chain Security and Industrial Policy

Provisions that protect and secure US Information and Communications Technologies (ICTs) were the third-largest category that included measures to prohibit federal agencies from purchasing ICTs from specific companies and promote the creation of an ICT-industrial policy. Supply-chain security and the need to develop an ICT-industrial policy gained prominence because of 5G and the Chinese-based company Huawei's dominance in the 5G supply-chain marketplace. This raised national-security concerns about the security and integrity of data flowing over networks with

Huawei technology and Huawei's ability to intercept or disrupt data and services at the request of the Chinese government. [33] Since then, Members of Congress have included provisions in NDAAs and passed similar bills to "clean" US networks of Huawei technology and other companies owned and operated by nation-state adversaries. [34] Yet, American and European companies lag behind Huawei in 5G technology and therefore lack a reliable alternative to replace Huawei; [35] an issue that transcends 5G technology and pervades other ICT markets and supply chains. [36] As a result, Congress has debated about how to create a new industrial policy that would invest federal funds into ICT companies to create a friendly competitor to Chinese businesses. However, the past two NDAAs show that Congress has ended this debate and inked a 21 st -century industrial policy whose origin centers on national security.

From FY 2017 to FY 2019, these provisions focused on protecting DoD's ICT supply chain from foreign-owned technology and establishing stronger information-sharing capabilities within intelligence agencies. [37] These NDAAs also included significant laws to prohibit foreign companies' influence in US markets. For example, the Foreign Investment Risk Review Modernization Act of 2018 was included in the FY 2019 NDAA and expanded the Committee on Foreign Investment in the United States' scope to address additional national security concerns, such as the supply-chain integrity of ICTs. [38]

Beginning in the FY 2020 NDAA, Members of Congress included provisions to incentivize domestic production of ICTs to wean US businesses and agencies off foreign-owned hardware and software. In fact, the FY 2021 NDAA included the new title, "Creating Helpful Incentives to Produce Semiconductors for America." Examples of provisions that fell within this title included:

- a report on how to increase investments in the "industries of the future;" [39]
- a trust fund within the Treasury Department to provide grants to promote and deploy 5G technology; [40]
- a public-private partnership to provide incentives (e.g., grants) to a consortium of companies to develop and produce microelectronics; [41] and
- federal financial assistance to incentivize investment in US semiconductor manufacturing, among others. [42]

While increased federal investment into ICTs is needed and has precedent, [43] Members of Congress must consider other areas of an industrial policy that may not fall squarely within the NDAA. For instance, the CSC detailed a series of recommendations on expanding the roles of the United States Agency for International Development, the Export-Import Bank, the Commerce Department, and the US International Development Finance Corporation to implement a whole-of-government approach to creating an industrial policy. [44]

Critical Infrastructure Protection, Election Security, and DHS' Cyber Mission

In addition to creating an industrial policy, Congress has used the NDAA to protect domestic critical infrastructure, secure election systems, and empower DHS' Cybersecurity and Infrastructure Security Agency (CISA). While these provisions are limited in number compared to other categories, they have significant implications in shaping US cybersecurity policy.

Although DoD does have a role in protecting domestic critical infrastructure from attacks, civilian agencies (known as Sector-Specific Agencies or Sector Risk Management Agencies) are primarily responsible for the day-to-day partnerships with private critical infrastructure partners. To further empower this partnership, Congress included key recommendations from the CSC to secure critical infrastructure from cyber threats. This included redefining the roles and responsibilities of sector-specific agencies who oversee the 16 critical infrastructure sectors; [45] creating a plan that would maintain and restore the economy in the face of a significant event (e.g., cyberattack); [46] and strengthening and institutionalizing DoD and other federal agencies cybersecurity initiatives with private partners. [47]

Election security also garnered significant attention among Members of Congress, with 11 provisions included in the past five NDAAs and a new title in the FY 2020 NDAA called "Election Matters." These provisions examined how the National Guard could assist states in securing election systems; [48] enabled information sharing with state election officials; [49] and created a strategy for countering Russian cyber threats to US elections. [50]

DHS' CISA also saw a surge of cyber-related provisions in FY 2021 compared to previous years mainly because it was created at the end of 2018 and due to a series of CSC recommendations that sought to strengthen its authorities. In fact, the FY 2021 NDAA was the first time in the past five NDAAs that Congress included a title called "Homeland Security Matters." These provisions gave CISA the ability to:

1. issue subpoenas to internet-service providers so that they can identify a company that may have a cyber vulnerability; [51]
2. conduct threat hunting operations on federal networks; [52] and
3. place cybersecurity coordinators in each state to improve federal relations with state and private partners, among other things. [53]

The 2021 NDAA also creates an office within CISA to convene federal agencies and private partners to develop joint cyber planning operations for protecting and responding to malicious cyber incidents. [54] As noted previously, this could impose consequences on cybercriminals and other malicious actors by taking down the infrastructures they use to perpetrate their crimes and acts.

The culmination of these provisions has the potential to transform public-private partnerships, solidify state and federal cooperation to protect elections, and enable CISA to perform its duties.

With Congress passing limited cyber legislation, Members should weigh the pros and cons of either including additional non-DoD cybersecurity provisions in future NDAAs or creating a cyber-omnibus bill to take a holistic approach to cybersecurity.

The SolarWinds hack, the Microsoft Exchange Servers vulnerability, and the relentless ransomware epidemic illustrate the need for Congressional action, but Congress must consider the best approach to enact legislation. Congress should weigh whether to include additional cyber-related categories in future NDAAs or create a cyber-omnibus bill so all agencies are provided with authorities and resources to deter and respond to cyber incidents.

The NDAA Approach

Congress sent about two dozen cyber-related bills to the Oval Office over a four-year time-period, which contained additional cyber provisions within them. Yet, this pales in comparison to the near 300 cyber provisions included in the past five NDAAs, with a hundred in the past NDAA alone. The FY 2021 NDAA was unique among others due to three new sections, which expanded the type of cyber provisions typically seen in an NDAA—Creating Helpful Incentives to Produce Semiconductors for America, Cyberspace-Related Matters; and Homeland Security Matters. As noted, the CSC was responsible for over 20% of the FY 2021 NDAA's cyber-related provisions, many of which fell within those three titles. With the CSC renewed for another year and advancing much-needed old and new recommendations to fill policy gaps, these and additional new titles may be included in the FY 2022 NDAA.

Congress should therefore not shy away from including other cybersecurity matters that are not directly related to the DoD. With ransomware and other forms of cybercrime at an all-time high, Congress should consider creating a new title in the FY 2022 NDAA called "Cybercrime Related Matters." Members could then include provisions that would provide additional funds to states and locals to enhance their digital forensic capabilities, improve assistance awarded to cybercrime victims, transform cybercrime reporting, and provide aid to US allies to bolster their criminal justice systems to investigate cybercrime cases, in addition to the CSC cybercrime recommendations. [55]

However, Congress should consider the pros and cons of using the NDAA to shape US cybersecurity policy. It is possible that there are limited cons and that the NDAA is simply a legislative means to an end. Yet, there may be limitations to thinking about cybersecurity through the defense bill and a national security lens, rather than an economic or innovative one. In other words, should the US

ICT-industrial policy strategy, for example, be grounded in a larger infrastructure package? Should filling the cybersecurity workforce gap be part of a 21st-century workforce bill? These types of bills will face political difficulties, and it is therefore understandable that they are included in a bill that has a perfect batting record for passing both congressional chambers over the past 50 years. But congressional members should then work together to overcome committee jurisdictional issues to include provisions in the NDAA that do not have a nexus to the DoD or national security, which will enable a holistic approach to US cybersecurity.

The Cyber-Omnibus Bill Approach

If Congress is already keen on including non-DoD provisions in the NDAA, they should consider the potential benefits of creating a cyber-omnibus bill. A cyber-omnibus bill would allow Congress to think about cybersecurity through a holistic approach by creating provisions that complement each other with a whole-of-society lens. For instance, such a bill could enumerate and resource a cyber bureau within the State Department, [56] de-conflict its mission with DoD, and provide resources to FBI attaches to support overseas cybercrime efforts. It could also ensure that states and civilian agencies are provided the resources to prevent, respond to, and investigate cyber incidents to lessen the burden placed on DoD assets, like the National Guard.

This legislative approach would also allow for commensurate resources to be allocated to civilian agencies who are responsible for partnering with private companies to protect the US against cyberattacks. Currently, the DoD's cyber operation budget is higher than CISA, the FBI, and the Justice Department's National Security Division combined. [57] DoD's cyber-related budget is also "nearly 25% higher than the total going to all civilian departments, including the departments of Homeland Security, Treasury, and Energy." [58] Further, some of the provisions included in the NDAA are unfunded mandates. Congress, for example, did not appropriate funds to implement the industrial policy it created in the 2021 NDAA. [59] Ensuring that the agencies responsible for helping state, local, private, and international partners prepare for and recover from cyber incidents is equally important as resourcing DOD's cyber operations and necessary for a complete cyber deterrence strategy.

Conlusion

Congress has used the NDAAs to pass important cybersecurity legislation, but Members must be aware of the importance of non-national security cybersecurity issues that tend to not be included in the NDAA. To be sure, a new legislative package would cause congressional jurisdiction headaches, which may outweigh any cons of relying on the NDAA to pass cyber-related legislation. Yet, the recent nation-state and cybercriminal activities taken against the United States and private companies show the need for Congress to use any means necessary to pass a wide range of cyber-related bills, with adequate resources provided to agencies, to bolster areas of US cybersecurity strategy that have been ignored thus far.

TOPICS

ENDNOTES

1. Miller, Maggie. "DHS Secretary Mayorkas announces new initiative to fight 'epidemic' of cyberattacks." *The Hill*, 25 Feb. 2021, https://thehill.com/policy/cybersecurity/540549-dhs-secretary-mayorkas-announces-new-initiative-to-fight-epidemic-of. Accessed 12 Mar. 2021.

2. "Group-IB: ransomware empire prospers in pandemic-hit world. Attacks grow by 150%." *Group-IB*, 4 Mar. 2021, https://www.group-ib.com/media/ransomware-empire-2021/. Accessed 12 Mar. 2021.

3. "Cyber Threats 2020: A Year in Retrospect." *PWC*, 2021. https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf. Accessed 12 Mar. 2021.

4. Cybersecurity Infrastructure Security Agency, US Department of Homeland Security. "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data." 10 Dec. 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-345a. Accessed 12 Mar. 2021.

5. "Cyber Threats 2020: A Year in Retrospect." *PWC*, p.26, 2021. https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf. Accessed 12 Mar. 2021.

6. Smith, Zhanna Malekos and Lostri, Eugenia. "The Hidden Costs of Cybercrime." *McAfee*, Dec. 2020. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 12 Mar. 2021.

7. Greenberg, Andy. "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say." *Wired*, 08 Feb. 2021. https://www.wired.com/story/oldsmar-florida-water-utility-hack/. Accessed 12 Mar. 2021.

8. Europol. "World's Most Dangerous Malware Emotet Disrupted Through Global Action." 27 Jan. 2021. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action. Accessed 12 Mar. 2021.

9. Office of the Governor, Louisiana. "Gov. Edwards Activates State Resources to Assist With Ongoing Cybersecurity Incident." 24 Jul. 2019. https://gov.louisiana.gov/index.cfm/newsroom/detail/2085. Accessed 12 Mar. 2021. Garcia, Michael. "Mobilizing the National Guard to Secure U.S. Elections." *Net Politics*, Council on Foreign Relations, 27 Feb. 2020. https://www.cfr.org/blog/mobilizing-national-guard-secure-us-elections. Accessed 12 Mar. 2021.

10. Garcia, Michael and Pat Shilo. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 116th Congress." *Third Way*, 10 Feb. 2021. https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-116th-congress. Accessed 12 Mar. 2021.

11. This does not include provisions related to ICT-industrial policy. Garcia, Michael and Pat Shilo. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 116th Congress." *Third Way*, 10 Feb. 2021. https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-116th-congress. Accessed 12 Mar. 2021.

12. Garcia, Michael and Pat Shilo. "Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 116th Congress." *Third Way*, 10 Feb. 2021. https://www.thirdway.org/memo/taking-action-on-cyber-enforcement-assessing-us-legislative-progress-in-the-116th-congress. Accessed 12 Mar. 2021.

13. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1752, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

14. US Cyberspace Solarium Commission. "NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission." 2 Jan. 2021. https://www.solarium.gov/press-and-news/ndaa-override-press-release. Accessed 12 Mar. 2021.

15. United States, Congress, House of Representatives, United States Code. P.L. 114-328. Title IX, section 923, 23 Dec. 2016. https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf. Accessed 12 Mar. 2021.

16. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1644, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021. and United States, Congress, House of Representatives, United States Code. P.L.116-92, Title XVI, section 1635, US Congress, 20 Dec. 2020. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

17. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1648, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title XVI, section 1636, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

18. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1638, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021.

19. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1725, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

20. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1729, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

21. Garcia, Michael. "Follow the Money: Few Federal Grants are Used to Fight Cybercrime." *Third Way*, 16 Feb. 2021. https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime. Accessed 12 Mar. 2021.

22. Examples include United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1651, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1739, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021. United States, Congress, House of Representatives. United States Code. P.L. 115-232. Title XVI, section 1638, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021.

23. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XXXI, section 3131, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

24. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title XVI, section 1648, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

25. United States Code. P.L. 115-232. Title XII, section 1281, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021.

26. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title XII, section 1246, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

27. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title X, section 1073, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

28. United States, Congress, House of Representatives, United States Code. P.L. 114-328. Title XVI, section 1654, 23 Dec. 2016. https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1641, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives. United States Code. P.L. 115-232. Title XVI, section 1636, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021.

29. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title LXVII, section 6729, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XII, section 1260F, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

30. United States, Congress, House of Representatives. United States Code. P.L. 115-232. Title XVI, section 1654, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021.

31. This provision was counted under "DHS Cyber Mission." United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1715, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

32. Garcia, Michael. "Follow the Money: Few Federal Grants are Used to Fight Cybercrime." *Third Way*, 16 Feb. 2021. https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime. Accessed 12 Mar. 2021.

33. Shepardson, David. "Five Chinese companies pose threat to U.S. national security – FCC." *Reuters*, 12 Mar. 2021. https://www.reuters.com/article/usa-china-tech-idINKBN2B5022. Accessed 16 Mar. 2021.

34. United States, Congress, House of Representatives. United States Code. P.L. 116-124. 12 Mar. 2020. https://www.congress.gov/bill/116th-congress/house-bill/4998. Accessed 16 Mar. 2021.

35. US Cyberspace Solarium Commission. "Building A Trusted ICT Supply Chain: CSC White Paper #4." Oct. 2020. https://drive.google.com/file/d/1ef096fPx5WkOxTiFFY1r5y3lFqdit00C/view. Accessed 16 Mar. 2021.

36. US Chamber of Commerce. "Understanding US-China Decoupling: Macro Trends and Industry Impacts." 2021, P.34-35. https://www.uschamber.com/sites/default/files/024001_us_china_decoupling_report_fin.pdf. Accessed 16 Mar. 2021.

37. See for example: United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1696, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives. United States Code. P.L. 115-232. Title XVI, section 1655, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title II, section 254, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title LVII, section 5705, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XVI, section 1634, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021.

38. United States, Congress, House of Representatives. United States Code. P.L. 115-232. Title XVII, section 1701, US Congress, 13 Aug. 2018. https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf. Accessed 12 Mar. 2021.

39. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XCIV, section 9412, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

40. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XCII, section 9202, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

41. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XCIX, section 9903, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

42. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XCIX, section 9902, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

43. According to the US Cyberspace Solarium Commission, "Congress created and appropriated funding for an industry-led consortium called SEMATECH,161 a name derived from "semiconductor manufacturing technology," in the National Defense Authorization Act (NDAA) of Fiscal Years 1988 and 1989; to encourage the U.S. semiconductor industry to conduct research and development (R&D) focused on advanced semiconductor manufacturing techniques in order to secure the United States' future commercial and defense needs." US Cyberspace Solarium Commission. "Building A Trusted ICT Supply Chain: CSC White Paper #4." Oct. 2020., P.28. https://drive.google.com/file/d/1ef096fPx5WkOxTiFFY1r5y3lFqdit00C/view. Accessed 16 Mar. 2021.

44. The US Cyberspace Solarium Commission created several recommendations that call on these agencies to have a proactive role in the US ICT industrial policy. US Cyberspace Solarium Commission. "Building A Trusted ICT Supply Chain: CSC White Paper #4." Oct. 2020. https://drive.google.com/file/d/1ef096fPx5WkOxTiFFY1r5y3lFqdit00C/view. Accessed 16 Mar. 2021.

45. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XC, section 9002, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

46. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XCVI, section 9603, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

47. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1728, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

48. United States, Congress, House of Representatives, United States Code. P.L. 115-91. Title XIV, section 1638, 12 Dec. 2017. https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf. Accessed 12 Mar. 2021.

49. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title LXV, section 6506, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

50. United States, Congress, House of Representatives, United States Code. P.L.116-92, Title LXV, section 6504, US Congress, 20 Dec. 2019. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. Accessed 12 Mar. 2021.

51. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1716, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

52. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1705, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

53. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1717, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

54. United States, Congress, House of Representatives. United States Code. P.L. 116-283. Title XVII, section 1715, US Congress, 1 Jan. 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr. Accessed 12 Mar. 2021.

55. US Cyberspace Solarium Commission. "Transition Book for the Incoming Biden Administration: CSC White Paper #5." Jan. 2021, P.17. https://drive.google.com/file/d/1gEx3_3Dlo6eyXX9tia1SnZAJFwcxKlM8/view. Accessed 16 Mar. 2020.

56. United States, Congress, House of Representatives. "H.R.1251 - To support United States international cyber diplomacy, and for other purposes." 25 Feb. 2021. https://www.congress.gov/bill/117th-congress/house-bill/1251/cosponsors?s=1&r=3&overview=closed&searchResultViewType=expanded. Accessed 18 Mar. 2021.

57. Healey, Jason. "The Cyber Budget Shows What the US Values—And It Isn't Defense." *Lawfare*, 1 Jun. 2020. https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense. Accessed 16 Mar. 2021.

58. Healey, Jason. "The Cyber Budget Shows What the US Values—And It Isn't Defense." *Lawfare*, 1 Jun. 2020. https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense. Accessed 16 Mar. 2021.

59. Will, Thomas. "FY21 NDAA Enacted: Science and Technology Policy Highlights." *American Institutes of Physics*, 9 Mar. 2021. https://www.aip.org/fyi/2021/fy21-ndaa-enacted-science-and-technology-policy-highlights. Accessed 16 Mar. 2021.