Submitted Statement for the Record of

Kathryn Waldron
Research Associate, National Security and Cybersecurity
R Street Institute

Kristen Nyman
Government Affairs Specialist
R Street Institute

Before the House Armed Services Committee
And its relevant subcommittees
House Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities
House Armed Services Subcommittee on Military Personnel
House Armed Services Subcommittee on Seapower and Projection Forces
House Armed Services Subcommittee on Tactical Air and Land Forces
House Armed Services Subcommittee on Strategic Forces
House Armed Services Subcommittee on Readiness

United States House of Representatives

Hearing on H.R. 2500 *National Defense Authorization Act for Fiscal Year 2020*

June 3, 2019

HEARING ON H.R. 2500 *NATIONAL DEFENSE AUTHORIZATION ACT* FOR FISCAL YEAR 2020, SUBMITTED STATEMENT OF KATHRYN WALDRON AND KRISTEN NYMAN

Chairman Smith, Ranking Member Thornberry and Members of the Committee:

Thank you for holding hearings to markup H.R. 2500 *National Defense Authorization Act* for Fiscal Year 2020 (NDAA). The purpose of this statement for the record is to highlight for the Committee a few issues that we believe warrant particular attention, including 5G competitiveness, supply chain integrity and workforce development.

We are part of the National Security and Cybersecurity policy team at the R Street Institute, a nonprofit, nonpartisan public policy research organization. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government in many areas, including national security policy.

As the Committee contemplates ways of ensuring national security through the 2020 NDAA reauthorization, we recommend that it consider addressing five policy areas discussed in detail below: supply chain security, security implications of 5G, election security, the prospect of a national space force and general cybersecurity. We hope you will find these materials helpful as you consider the reauthorization of the 2020 NDAA.

I. National Security Implications of Supply Chain Vulnerabilities

Ensuring American national security means, in part, ensuring supply chain integrity. As the Committee knows, modern conflict is no longer limited to the kinetic warfare of the past. U.S. adversaries seek to exploit American weaknesses wherever they can—developing robust capabilities to engage in a range of destructive cyber activities targeted at both U.S. government agencies and critical industries. A cyberattack against the American electrical grid or command-and-control communications systems during a crisis could have devastating consequences if a supplier for these systems lacks sufficient cybersecurity protections, or worse, willingly provides a platform of attack. Therefore, it is vital that the companies in the supply chains for key military and civilian systems in the public sector, as well as critical infrastructure and key resources in the private sector, are thoroughly vetted to prevent incorporating any weak links that could be exploited in a time of crisis.

Last year's John S. McCain National Defense Authorization Act demonstrated a growing awareness of the importance of supply chain security by banning federal government use of certain products from Chinese firms such as Huawei and ZTE.[1] However, Huawei and ZTE are not the only companies that pose a threat to the federal government's supply chain. Russian companies such as Kaspersky Lab, the Speech Technology Center and Chinese telecommunications supplier Lenovo are just some of the other companies that should be evaluated carefully from a cyber supply chain risk perspective. Each of these companies comes from a country whose legal structure gives government officials the authority to access data—and some of these companies even advertise

[1] H.R.5515, John S. McCain National Defense Authorization Act for Fiscal Year 2019, 115th Cong.

their closeness to their respective governments. (Kaspersky Lab ran a 2007 ad campaign in Japan that read, "A Specialist in Cryptography from KGB."[2])

We applaud the recent federal focus on identifying and better addressing certain supply chain vulnerabilities. In addition to banning Huawei and ZTE from federal government use, the signing of the SECURE Technology ACT created the new Federal Acquisition Security Council, comprised of members from a variety of federal agencies, including the Department of Defense. Additionally, a new ICT supply chain task force, with representatives from both public and private sectors, will hopefully foster the public-private dialogue needed to protect critical industries that serve the whole nation.

However, there is still more work to be done on this important issue. In our view, the United States "lacks a publicly available and clearly articulated, comprehensive, dynamic, prioritized and holistic assessment of: (1) what public and private sector assets it should protect from supply chain risk; (2) the supply chain threat actors who pose the greatest risk; (3) the malicious tactics, techniques and procedures that such threat actors use or are likely to use to accomplish their objectives; (4) the vulnerabilities that exist to U.S. information systems and devices; (5) the most effective and efficient defensive measures and mitigation strategies for thwarting adversaries and recovering from failed mitigation efforts; and (6) the metrics and measures that public and private sector entities should use to accurately assess the supply chain threat and the effectiveness of risk mitigation and recovery efforts put in place to address those threats."[3]

In order to better address the supply challenges that the United States faces, we recommend the NDAA require the Department of Defense to conduct a thorough security review of its entire supply chain. As Mike Gordon, deputy chief information security officer at Lockheed Martin, said last year, "Because of contract privity and competitive advantage, the tier one doesn't necessarily know who in the tier four is working on a particular program, and the government does not necessarily know that either."[4] We recognize that tackling such a vast network may seem like a monumental task; indeed, it will be complex and resource intensive. Nonetheless, it is crucial that the appropriate funding and resources for this audit be set aside in the 2020 NDAA. The longer government officials take to begin reducing key supply chain vulnerabilities, the more time criminal hackers and hostile nation-state actors will have to exploit these vulnerabilities, with potentially devastating results.

II. Election Security

With 2020 quickly approaching, election security should be a primary concern for lawmakers as they reauthorize the NDAA. In this section, we will describe some of the election vulnerabilities

[2] Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, June 24, 2018, p. 9. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyondunderstanding-russias-approach-to-cyber-enabled-economic-warfare.

[3] Paul Rosenzweig and Kathryn Waldron, "Broadening the Lens on Supply Chain Security in the Cyber Domain," R Street Institute, April 2019. https://www.rstreet.org/wp-content/uploads/2019/04/Final-No.-170.pdf.

[4] Justin Lynch, "Pentagon moves to secure supply chain from foreign hackers," *Fifth Domain*, October 21, 2018. https://www.fifthdomain.com/dod/2018/10/21/pentagon-moves-to-secure-supply-chain-from-foreign-hackers/.

made evident by Russian interference in the 2016 presidential election, identify additional security concerns unrelated to Russia, and provide election security recommendations from two perspectives—entities over which the government has jurisdiction and those over which political entities retain jurisdiction.

In the wake of the 2016 election, we have seen the impact that coordinated attempts by foreign hostile nations can have on the American electoral system. Department of Justice Special Counsel Robert Mueller called the attacks "multiple and systematic." Indeed, the 2016 Russian election hack utilized at least three tactics: online propaganda, direct hacking of political entities and targeting of state election systems. Each of these tactics exposed unique vulnerabilities in the U.S. election system that this Congress must address before the 2020 election.

Online Propaganda

The Russian Federation was behind a large-scale disinformation campaign leading up to the U.S. presidential election in 2016. Russians were responsible for creating thousands of bots operating on Facebook, Twitter and Google. These bots shared paid and unpaid posts to millions of Americans, including commentary on political content, fictitious news stories and political advertisements. A Russian bot's page is indistinguishable from any other page in the eyes of the typical viewer, so these posts were shared and re-shared millions of times by legitimate profiles. While it is difficult to measure the exact impact this disinformation campaign had on the outcome of the election, to some degree the very nature of the attack itself achieved the objective to undermine confidence in the American democratic election system.

Preventing this style of attack is difficult because it requires a sophisticated level of training and situational awareness, primarily on the part of private citizens and private companies. In order for Congress to enhance cybersecurity in the election system, it must work with industry leaders and stakeholders to outline standards and create tools for the private and public sectors alike. An appropriately aggressive level of cooperation between government entities and large technology companies such as Twitter and Facebook, in accordance with the Constitution and laws of the United States, is paramount to securing American elections.

Direct Hacking of Political Entities

As we now know, the Russian Federation also hacked various systems in order to obtain emails and other documents that it later disclosed publicly via a variety of means in an effort to influence the outcome of the presidential election. Congress must find a way—consistent with the Constitution—to work with political candidates and organizations to protect sensitive communications and data. In an NDAA context, this could mean funding for enhanced cybersecurity initiatives and better-enforced security standards.

Targeting State Election Systems

The Department of Homeland Security (DHS) identified 21 states that the Russians targeted directly during the 2016 election. The DHS has assessed that there was no tampering with actual votes, but in at least one case in the state of Illinois, the Russians managed to access personal information about voters. DHS Cyber Division Acting Director Dr. Samuel Liles expressed to the Senate Select Committee on Intelligence that the other 20 states were likely scanned for vulnerabilities and likened the effort to "a thief walking through your neighborhood to see if anyone is home."

In addition to issues related to the Russian 2016 election hack, a full view of election security factors should include those that have not yet been exploited, but are vulnerable at present and could be the subjects of future attacks if left unaddressed. We describe a few of these below.

Registration

When new voters register, they typically do so through a third-party organization or entity separate from the one that maintains the voter database—leaving multiple points of entry and thousands of employees and volunteers vulnerable to exploitation.[5] Many of these organizations lack sophisticated infrastructure at the grassroots level to ensure that voter data is secure.

Congress should consider funding for a central clearinghouse to provide guidance on training, streamlining, modernizing and securitizing the election registration system.

Database Maintenance

As is required by the Help America Vote Act of 2002 (HAVA) each state maintains a database of voters that contains their personal information. HAVA was created before encryption technology was widely used, so the act does not require that any data in transit be encrypted. The act does, however, require the data to be housed in a single, uniform, official, centralized, interactive and computerized manner that is defined, maintained and administered at the state level—leaving all of the information a hacker could want in one convenient location. The act also does not require that the system be segregated from others—say, for example, business filings, which are also typically handled by each state's secretary of state. Therefore, if there were to be a simple IT department error in granting access, the entire database would be compromised.

Congress should consider setting standards and funding a central clearinghouse to assist states in creating initiatives to train state-level Departments of State on cybersecurity best practices for election database management.

Precinct Voting Books

Another feature of HAVA is the use of precinct voting books to identify the correct ballot for each voter, based on the geographic location of their registered address and their party affiliation. On election day, access to this personal voter data is typically in the hands of part-time employees or poll workers who do not have access to the cybersecurity training that full-time government employees have.

[5] Paul Rosenzweig, "Thinking Analytically About Electoral Security," *R Street Institute,* April 2018. https://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/Final-140.pdf

Congress should fund a central clearinghouse to assist states in identifying threats, and training and creating standards to ensure the highest level of election security across the country.

Additional Electoral Concerns

R Street Senior Fellow Paul Rosenzweig outlined five major election security concerns as follows:[6]

> The registration data for voters could be manipulated and degraded, rendering it unreliable and inaccurate, thereby creating questions as to who is an eligible voter;
>
> Voter rolls could be amended or supplemented to add or delete potential voters;
>
> The entire voting database could be encrypted by a ransomware attack on the day before an election, rendering it unusable;
>
> Precinct-level vote books could be likewise degraded, destroyed or rendered unavailable for use;
>
> The actual voting totals in individual machines could be altered; and
>
> The broader voting tallies across county- or state-level organizations could be manipulated via interception and modification during the course of transmission to state authorities.

The bottom line, as Rosenzweig puts it, is:

> The electoral infrastructure system is severely under-resourced;
>
> A lack of standards or best practices creates a heterogenous attack surface;
>
> Electoral infrastructure lacks a central clearinghouse for information regarding threats and vulnerabilities.

Congress should consider funding the aforementioned initiatives to ensure that anyone who handles personal voter data is well-equipped to detect and combat malicious activity.

III. Security Implications of 5G

The opportunities presented by 5G technologies are unprecedented and far-reaching. These capabilities will profoundly enhance artificial intelligence, revolutionize the medical field and fundamentally alter communications infrastructure as we know it. There are two perspectives from which Congress must look at this issue: competitiveness and security.

As with any emerging technology, it is essential that the United States be at the forefront of the 5G race. Currently we are being outpaced by China because their full attention (and a large chunk of their budget) is devoted to developing this and other emerging technologies—not to mention

[6] Ibid.

they have three times the population size of the United States.[7] Competitiveness with China and other emerging technological giants presents a serious national security concern for the United States.[8]

R Street Director of Technology and Innovation Policy Charles Duan puts it this way:[9]

> To ensure cybersecurity in a world of ubiquitous devices, an essential component is competition among firms up and down the vertical chain. Competition promotes better cybersecurity in at least two ways. First, multiple studies show that competition encourages firms to improve their products on multiple vectors including cybersecurity. Second, competition avoids a situation that security experts call a "monoculture," which increases vulnerability to severe cyberattacks.
>
> Congress should thus approach invocations of cybersecurity threats with a dispassionate eye, considering the consequences for competition of imposing restraints on trade in the name of security. By the same token, to the extent that Congress considers measures to increase security, its first line of approach should be reducing entry barriers to new startup firms in order to increase competition.

When reauthorizing the NDAA, Congress should take steps to ensure that 5G is a priority for the federal government and the private sector. Funding should focus on making sure that the U.S. is the leader in building and operating secure and reliable 5G networks by leveraging our existing telecommunications infrastructure and supporting innovation through free-market competition A substantial investment in 5G infrastructure would maintain the United States' competitive advantage and strong global security presence.

When looking to secure the new network environments that a 5G world with new components like micro- and pico-cell architecture and edge-based cloud computing will create, Congress might consider the following components of a 5G security policy:

> *Edge-to-edge securitization*: All connections to the enterprise ecosystem must be identified and criticality rated to ensure that network access requests can be authenticated.
>
> *New techniques to secure systems*: Network segmentation is a tried and true cybersecurity technique, but in order to enhance security for the 5G environment, it is important to combine it with other techniques, such as network slicing, in order to secure edge-to-edge, hybrid and co-managed systems.

[7] Charles Duan, "Why China IS Winning the 5G War," *The National Interest*, March 14, 2019. https://www.rstreet.org/2019/03/14/why-china-is-winning-the-5g-war-2/.

[8] Charles Duan, "U.S. Patents and Competitiveness with China," *R Street Institute*, February 2, 2019. https://www.rstreet.org/2019/02/27/u-s-patents-and-competitiveness-with-china/.

[9] Submitted Statement of Charles Duan, Senate Committee on the Judiciary, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation," 116th Congress, May 14, 2019. https://www.rstreet.org/2019/05/23/5g-national-security-concerns-intellectual-property-issues-and-the-impact-on-competition-and-innovation-submitted-statement-of-charles-duan/.

> *Security technology integration*: Due to incredible data transmission speeds that will come with 5G, it will be more important than ever for systems to be deeply integrated in order to share threat intelligence, correlate event data, inspect encrypted data and automate incident responses. It will be necessary to rely heavily on automation, machine learning and other artificial intelligence techniques to create a brand-new, adaptable security infrastructure.

In order to prepare adequately for a 5G world, Congress must employ strategies it has never legislated on previously and that very few people in the government are working with consistently. Securing the 5G network will be an arduous but necessary task, and it will require a sizeable investment from Congress.

IV. Testing the Cybersecurity of Existing DOD Systems

Government officials have shown increased awareness of cybersecurity's importance. The DOD has issued or updated guidance regarding weapon systems' cybersecurity fifteen times in the past four years alone.[10]

However, merely creating (frequently changing) guidelines is not sufficient to ensure adequate cyber defenses. A report released last year by the Government Accountability Office (GAO) revealed that America's weapon systems are actually permeated with cyber vulnerabilities. Weaknesses can be as basic as poor password management and unencrypted communications. In the GAO report, testers guessed one administrator's password in only nine seconds. Testers also managed to surreptitiously observe remote monitors, send employees irritating pop-up messages, change or delete data, and even cause systems to shut down entirely. In one instance, a two-person test team hacked its way to full control of a system in just one day.[11]

When GAO officials revealed these flaws, DOD officials pointed out the list of security controls they had already implemented.[12] But mere compliance with static guidelines is insufficient. The reality is that America's adversaries are constantly evolving, developing new types of malicious cyber actions. When one security control is put in place, adversaries will switch to other tactics, techniques and procedures, seeking and exploiting other vulnerabilities. The DOD must match, and indeed supersede, the agility of adversaries in the cyber realm.

Instead of creating yet another best practices list, we recommend that through the NDAA Congress authorize funding and resources for the DOD to enact systematic "red-teaming" tests of all major systems, both current and in production. Red-teaming, in which a designated group "attacks" a system the way a real adversary would, would enhance the ability of DOD officials to determine where the most significant vulnerabilities in each system lie.

[10] Derek B. Johnson, "GAO: DOD weapons systems easy to hack," *FCW*, October 9, 2018. https://fcw.com/articles/2018/10/09/gao-pwns-dod.aspx.

[11] "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," Government Accountability Office, October 9, 2018. https://www.gao.gov/products/GAO-19-128.

[12] "Weapons System Cybersecurity," Government Accountability Office, p. 19.

In order to both identify and address cyber vulnerabilities, the DOD must be able to both recruit and retain a highly capable cyber workforce. In addition to understanding cybersecurity, DOD cybersecurity experts must also know how the agency's acquisition process works and understand the technical aspects of each weapon system's various components. But despite the crucial role these experts play, DOD salaries for cybersecurity experts are not competitive compared to those offered by private companies. According to Glassdoor, the average DOD cybersecurity analyst makes only $72,000 per year.[13] These experts would be far better paid in the private sector, where top analysts often earn compensation of $200,000 per year or more.[14] Therefore, we also recommend that the NDAA authorize funding that could be used to provide benefits and other financial incentives for IT professionals. The inability to hire and retain cybersecurity experts is a serious risk to U.S. national security.

V. National Space Force

The United States relies heavily on vulnerable space-based technical assets to conduct essential military and civilian affairs. As a result, the United States must take appropriate steps to protect and defend those assets from kinetic cyberattacks and other malicious activities by a range of threat actors. During the Cold War, space capabilities were primarily concentrated between the governments of the United States and the Soviet Union; now those capabilities have proliferated to many other nations. Between 1991 and 2016, 43 percent of new satellites were owned by countries outside of the United States and Russia, notably from China, Japan, India and Europe.[15] The development of satellite technology brings several military advantages. Satellites make it easier to conduct command-and-control (C2) activities and deliver precision-guided munitions, the use of which by the U.S. military has grown tremendously since the 1991 Gulf War. Satellites are also used for navigation; intelligence gathering; and for early warning against strategic attack by, for example, ICBMs. The use of satellite communication systems (SATCOM) is so expansive that the DOD often must lease bandwidth from private operators in order to conduct military operations.[16]

Satellites face many security risks. Perhaps the most obvious threat is physical destruction—either by an adversary destroying satellite ground stations through conventional weapons or destroying satellites themselves using anti-satellite missiles. Satellites can also be damaged or destroyed using high-powered lasers, microwaves or electromagnetic pulses. In other cases, it is not the satellite's physical existence that is threatened, but its functional capability. Jamming or spoofing radio frequency signals can interfere with a satellite's ability to send and receive data. For example, Russia has launched four satellites suspected to have the capacity to physically attack or disable

[13] "US Department of Defense Cyber Security Analyst Salaries," Glassdoor, March 29, 2019. https://www.glassdoor.com/Salary/US-Department-of-Defense-Cyber-Security-Analyst-Salaries-E14798_D_KO25,47.htm.

[14] Steve Morgan, "Top Cyber Security Salaries In U.S. Metros Hit $380,000," *Forbes*, Jan 9, 2016. https://www.forbes.com/sites/stevemorgan/2016/01/09/top-cyber-security-salaries-in-u-s-metros-hit-380000/#666fd647ef87.

[15] Todd Harrison et al. "Escalation and Deterrence in the Second Space Age," Center for Strategic and International Studies, October 3, 2017, p. 6. https://www.csis.org/analysis/escalation-and-deterrence-second-space-age.

[16] Harrison, pp.6-7.

U.S. satellites. China tested anti-satellite missiles in 2007, 2010 and 2013. And both countries are developing tools such as lasers and jammers that could interfere with a satellite's performance.

But one of the most dangerous threats satellites face is from malicious cyber actions. Satellites offer hackers a variety of access points, including the antennas on both satellites and their ground stations and user terminals here on earth. Malicious cyber actions can range from stealing data, to sending fake or corrupt data, to a complete shutdown of all satellite operations. Such malicious cyber actions can be very hard to detect, and even when discovered, attribution to a particular threat actor can be difficult. This attribution problem weakens deterrence and can make it hard to hold malicious actors responsible.

We have already seen malicious cyber actors target U.S. satellites. Satellites operated by the U.S. Geological Survey and NASA were compromised in 2007 and 2008; the hackers used a ground station in Norway to interfere with satellite communications for several minutes.[17] In another cyber event, hackers gained control of systems at NASA's Jet Propulsion Laboratory.[18] And in 2014, hackers compromised the National Oceanographic and Atmospheric Administration's (NOAA) weather and satellite systems.[19]

Thus, it is imperative that the 2020 NDAA authorize adequate funding to improve our current defenses in space significantly and then closely monitor the DOD's use of such funds. Previous space-related projects have suffered from cost overruns and delays. As an example, by 2017, the Air Force Space Command's Advanced Extremely High-Frequency satellite program's costs had exceeded its budget by 118 percent, while the Space Based Infrared System program's costs exceeded its original budget by 300 percent.[20] Lack of clarity regarding the size of the current space-focused workforce as to exactly how defenseless our space assets are thus leaves in question whether a full-born "Space Force" is indeed needed, or whether some smaller space corps might serve better. Regardless, it appears that the militarization of outer space is imminent, if not already here. If the United States wants to retain its position as a global leader, the NDAA must provide sufficient funding for further development of U.S. military capabilities in space.

We would like to thank the Committee for its attention to the matters presented above. If we or our colleagues at the R Street Institute can be of any assistance to members of the Committee, please feel free to contact us.

[17] John Leyden, "Inside the mysterious US satellite hacking case," *The Register*, November 21, 2011. https://www.theregister.co.uk/2011/11/21/us_sat_hack_mystery/.

[18] Kim Zetter, "Report: Hackers Seized Control of Computers in NASA's Jet Propulsion Lab," *WIRED*, March 1, 2012. https://www.wired.com/2012/03/jet-propulsion-lab-hacked/.

[19] Doyle Rice, "China hacks into U.S. weather satellite network," *USA Today*, November 12, 2014. https://www.usatoday.com/story/weather/2014/11/12/china-weather-satellite-attack/18915137/.

[20] "Space Acquisitions: DOD Continues to Face Challenges of Delayed Delivery of Critical Space Capabilities and Fragmented Leadership," Government Accountability Office, May 17, 2017. https://www.gao.gov/assets/690/684664.pdf.

Kathryn Waldron

Research Associate, Cybersecurity and National Security

kwaldron@rstreet.org

Kristen Nyman

Government Affairs Specialist

knyman@rstreet.org