DEPARTMENT OF THE ARMY
DEPARTMENT OF SOCIAL SCIENCES
UNITED STATES MILITARY ACADEMY
BLDG 607, LINCOLN HALL
WEST POINT, NY 10996

MADN-SOC 6 NOVEMBER 2021

MEMORANDUM FOR Chris Inglis, National Cyber Director

SUBJECT: Defending Critical Infrastructure and Bolstering Cyber Defense

1. **Issue**:

This roundtable is interested in reinforcing the domestic partnership between the public and private sectors, in protecting the nation against threats to vital supply chains and critical infrastructure sectors, in educating the population on basic cyber literacy, and in establishing international guidelines for the standardization of secure supply chain management with our partner nations.

2. **Strategic Analysis:**

Cyberspace presents a uniquely challenging environment for American national security and foreign policy. New digital technologies emerge as opportunities for social innovation and devastating cyber warfare. Developments in artificial intelligence and machine learning challenge conventional frontiers of state surveillance and data management, while cloud computing simplifies operations, but simultaneously raises concerns as to the vulnerabilities of a cyber-attack on its reliant services. Revolutionary advancements in cyber technologies are accompanied by an equally concerning rise in newfound dangers associated with these technologies. What does it mean for rival state actors when our critical infrastructure sectors are overly reliant on cloud services? How should we enforce supply chain security around the world, protect our firms from cyber-attacks, and have our citizens educated on basic cyber literacy? In exploring potential solutions to these questions, we believe we are addressing the very future of American cybersecurity.

The United States must continue to take vigilant notice of relevant actors in the cyber domain today, particularly those in the public and private sectors, our state rivals and allied nations, and non-state actors. “Big tech” firms with sizable market shares, such as Microsoft, Apple, and Intel; energy companies that provide fuel and electricity; defense industries, such as Lockheed Martin; governmental agencies such as CISA and the Intelligence Community; all are key players in cyberspace today. While state rivals such as China, Russia, Iran, and North Korea pose significant threats to American cyber security today, our alliances in NATO and the Five Eyes provide us with a solid bulwark of cyber defense that we must actively seek to preserve, and strengthen, in the future. The underlying motives and actions of non-state actors, including cyber criminals, lone wolf activists, and individual open source developers, must also be carefully observed and understood in the context of protecting American interests in cyberspace. Intersecting across various domains, all of these actors constitute the landscape of international cyberspace today, and a clear definition of their roles and relationship with the United States will be critical to our national cybersecurity now and in the future.

MADN-SOC

SUBJECT: Defending Critical Infrastructure and Bolstering Cyber Defense

Certain trends have also emerged in the debate over cybersecurity in recent years, with particular salience attached to the issues of government oversight in U.S. cyberspace, global supply chain security for imported American technological products, and American power projection in the political, economic, and now cyber dimensions of Chinese-American power dynamics today. Indeed, the question arises as to whether the U.S. should pursue a policy of “cyber deterrence” in dealing with its adversaries, and actively explore the usage of cyber offensive and defensive capabilities for use in the future.

3. **Relevant National Interests:**

The United States government has a marked interest in securing a safe market for US companies and consumers. As global supply chains overlap to form a just-in-time delivery network and software dependencies weave a similar pattern, it is the government’s responsibility to mitigate threats to these support systems. Problems with either availability or security can decrease trust in the institutions meant to protect and uplift the economy, and earning consumer trust is necessary to support development in high-tech, research-based fields of technology.

The United States also wants to support nascent markets and developing economies join the world market in the digital revolution. The advances made in developed markets can be adopted by others to increase the pace of development for all nations. Creating an environment of partners with consensual interests and standards will serve as a counter to destabilizing forces in the global economy.

4. **Strategic Approach:**

This Committee hopes to foster the development of international security standards and global coordination between the United States and its economic partners in the world, while also reinforcing our own domestic security measures in order to ensure that our cybersecurity remains uncompromised. We place a particular emphasis on leading a global effort to strengthen the security of supply chains to critical infrastructure sectors within the United States and its trading partners, as well as educating our population in cybersecurity and basic cyber literacy. We believe that these objectives place both the long and short-term interests of American cybersecurity at heart, and will take steps to enforce cybersecurity domestically and internationally with different emphases on coordination, education, and novel standardization.

5. **Recommendation:**

Incentivizing Education to Build a Cyber Workforce:

i. State implementation of: primary and secondary-level government-designed education curriculums such as internet safety, password protection, and interactive modules appealing to these age groups; high-school level programs focused on introductory computer science language learning and speaker events with cyber experts incentivized by scholarships and research contests. These K-12 programs are intended to be marketed as critical for students' futures as global netizens.

ii. Government-sponsored college-level educational programs targeted towards cyber threats, including fellowship programs in cyber and intelligence spaces mirrored off of

the National Security Education Program for learning languages critical to national security and agency-sponsored certifications tailored to students involved in different educational concentrations, focusing on specific pressing threats (supply chains, ransomware, etc.). Incentives to partake in such a program include government-sponsored research opportunities or writing competitions and the granting of agency-approved certification for students who complete the programs.

Enforcing Domestic and International Supply Chain Security (GSOCC):

i. The foremost creation of a domestic agency that evaluates the supply chain security of American technology firms; its primary function will be to assign a security rating of four levels (Poor, Adequate, Satisfactory, Secure) to American tech companies outsourcing production overseas, especially those firms whose supply chains are linked to the 16 critical infrastructure industries as defined by CISA. This Agency will conduct a preliminary review of the 16 critical infrastructure sectors, rating their cyber security in terms of Least to Most Secure. After the initial ratings are deemed satisfactory, the Agency will be responsible for evaluating individual companies and their supply chains in terms of cybersecurity risk; such evaluations will ultimately allow for greater transparency of security measures between the public and private sectors. Under this inspection and review process, the integrity of American technology will remain secure while also ensuring system efficacy across the supply chain network itself.

ii. Trading partners and allies of the United States will be encouraged to adopt these guidelines and security standards as well, and foster a global network of Information Sharing Access Centers (Global ISACs) that serves to enhance overall supply chain security in the world.

iii. Each nation that adopts these standards will be labelled as Standard Compliant, becoming eligible to join the General Security Oversight Committee on Cybersecurity (GSOCC), the function of which is an international body designed to coordinate responses to supply chain threats, vulnerabilities, and vital information updates within respective cyber security agencies. GSOCC would further serve as an annual cyber security summit between member nations, emphasizing supply chain security and standard compliance, and extending its influence to the rest of the world.

Unified Cyber Intelligence Community:

i. Recommendation to closely monitor the status of two proposed Senate bills titled “Cyber Incident Reporting Act of 2021” and the “Cyber Incident Notification Act of 2021.”

1. These acts intend to mandate companies within the private sector and public infrastructure communities to report cyberattacks such as ransomware within a designated time period to CISA. If both of these acts fail to pass, then instituting an executive order to achieve parallel results constitutes the recommended course of action.
2. Consider requiring all organizations which work with the private sector and critical infrastructure communities to follow the same or similar mandates.

3. Require that the government protects the privacy rights of standard compliant reporters, rather than making these findings public and require a response from CISA to the reporter.
4. Mandate CISA to report attacks to the DoD, to determine appropriate responses.
5. Mandate periodic reviews from the Cyber Safety Review Board to ensure proper practice of CISA's handling of these mandatory reports to ensure that all party's interests and liberties are being considered and protected, while recommending change if they are not.

ii. Incentivize private sector participation in reporting by assuring the retention of contracts and support to companies who fall victim to cyberattacks and have followed all reporting and remedial guidelines. Agree to coordinate public statements with victim companies to reframe media narratives, ensuring all culpability is duly placed on cyber criminals rather than victim companies.

6. The point of contact for this memorandum is Cadet Captain Zachary Bolen at zachary.bolen@westpoint.edu or 913-704-9095.