QUESTIONS FOR THE RECORD
Suzanne Spaulding
Committee on Oversight & Reform
July 15, 2020, Hearing: "U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act."

Questions from Chairwoman Carolyn B. Maloney

1. Does the United States' risk for sustaining a major cyber incident increase when the country experiences other national crises like the coronavirus pandemic? How would having a National Cyber Director help to control the risk and decrease the likelihood that one national crisis leads to another?

The risk to the country of sustaining a major cyber incident does greatly increase when the country experiences other concurrent crises, but particularly in the case of the coronavirus pandemic where dependence upon the internet has vastly increased. The COVID-19 experience has underscored the importance of many of the Commission's recommendations.

- The broad-based effort required to address COVID-19 is similar to the broad effort required to address cyber risks and highlights the need for strategic leadership and strong coordination. This underscores the importance of the Commission's recommendation for a National Cyber Director to serve as the President's principal advisor on cyber issues.
- During catastrophic events such as the COVID-19 pandemic or a significant cyberattack, the United States must have a crisis management team and clear strategies in place ahead of time to coordinate an effective response, both at home and abroad. The pandemic has laid bare the limitations and interdependence of both the private sector and the government, highlighting that any successful management of a crisis—cyber or otherwise—will require a coordinated, well-planned, and shared response. The government, the private sector, and the public each have unique and shared responsibilities, and these groups must take the measures necessary to ensure their preparedness to quickly and seamlessly respond to a potential crisis. Ensuring that the federal government has clear plans, processes, and capabilities in place before an incident will significantly improve its capacity to aid in response to and recovery from a crisis.
- Today's circumstances validate the Commission's recommendation for the establishment of a National Cyber Director (NCD), who would act as the President's principal advisor for cybersecurity and related emerging technology issues. As the chief U.S. representative and spokesperson on cybersecurity issues, the NCD would head the development of the national cybersecurity strategy, lead joint interagency planning for the federal government's response activities to cyberattacks, coordinate the federal government's incident response activities related to cyber, and serve as the focal point for private sector leaders to engage the White House on cybersecurity issues.

The Commission also found these important lessons learned:

- First, as more and more businesses encourage or require their employees to work from home, in-home devices become critical nodes in enterprise networks. Home internet-of-things devices—and routers, in particular—are known to be an area of significant vulnerability.
    - The Commission therefore recommends that Congress pass an internet of things (IoT) security law that focuses on known problems, like routers, and mandating enduring security features, like unique passwords.
- Second, the increase in fraud and other malicious activity during the pandemic underscores the need to build capacity to combat opportunistic cybercrime.
    - The Commission therefore recommends that, in addition to strengthening the FBI's NCIJTF, Congress should provide grant funding through the Department of Justice's Office of Justice Programs to support nonprofits that assist law enforcement's cybercrime and victim support efforts:
- Third, the current crisis has highlighted the importance of the U.S. population's ability to separate fact from fiction in order to limit fear and save lives. It is imperative that the United States possess the capacity to identify threatening disinformation activities and promptly communicate them to both the platforms that enable the activities and the general public.
    - The Commission therefore recommends that Congress should fund the DoJ to provide grants, in consultation with the DHS and the National Science Foundation, to non-profit centers to identify, expose, and explain malign foreign influence campaigns to the American public while putting those campaigns in context to avoid amplifying them.
    - The Commission also recommends that Congress support the provision in the FY2020 National Defense Authorization Act that authorizes the Office of the Director of National Intelligence to establish and fund a Social Media Data and Threat Analysis Center (DTAC), which would take the form of an independent, nonprofit organization intended to encourage public-private cooperation to detect and counter foreign influence operations against the United States.
    - Additionally, the Commission recommends promoting and modernizing civic education and digital literacy as a way to grow societal resilience against information operations and instill a stronger sense of civic responsibility in our country. Information operations have been an area of concern pre-COVID, but the pandemic has made apparent that the American population is a vulnerable target at a time when they must instead be the first line of defense.
- Finally, certain aspects of the Commission's original report needed to be strengthened in light of the lessons being learned during the COVID-19 pandemic, particularly in response to the need to digitize critical services and do so securely in response to the imperative of social distancing, including incentivizing secure movement to the cloud and broader modernization in state, local, tribal, and territorial governments.

- The widespread disruption of the economy, highlights the importance of Continuity of the Economy planning to ensure the continuous flow of goods and services regardless of the cause of disruption. The disruptions to our supply chains from COVID-19 and the need to direct resources using Defense Production Act authorities, underscore the importance of both understanding where risks lie and having the requisite plans and authorities in place to direct resources in a national emergency.

2. What harm did the elimination of the Cybersecurity Coordinator role by then-National Security Advisor John Bolton do to our nation's cybersecurity readiness?

The decision to remove the White House Cybersecurity Coordinator position eliminated a key senior-level focal point for coordinating cybersecurity in the executive branch. Countering cyber risks requires effectively leveraging expertise, authorities, and resources of many agencies and the private sector. While individual agencies have continued to advance their cyber missions, there has been inadequate focus on strategic planning and coordination, leaving us less prepared to anticipate and respond to malicious cyber activity. This inadequacy is visible in four main ways:

- First, the federal government lacks consistent, institutionalized leadership in the White House on cybersecurity strategy and policy.
- Second, due to the absence of a consistent advocate, cybersecurity is inconsistently prioritized in the context of national security.
- Third, the United States lacks a coordinated, cohesive, and clear strategic vision for cyber.
- Fourth, the lack of centralized executive branch leadership complicates and prevents effective congressional oversight.

3. Would the size and placement of the Office of the National Cyber Director within the Executive Office of the President add a layer of bureaucracy, or would it enable the Director to reduce redundancies to make our cyber response more effective?

- The Commission recognized the need for a single individual at the highest level in the federal government and envisioned the National Cyber Director, and the accompanying office, as the executive branch structure that would address these needs in preparation for future challenges.
- Our recommendations are aimed at streamlining government strategy and action while consolidating oversight. Too many parts of government are currently pursuing objectives in cyberspace that are redundant or, worse, at cross-purposes. The National Cyber Director will bring coherence, speed, and agility to these too-often disconnected and sprawling efforts.
- In proposing the creation of a National Cyber Director, we sought to establish this coordinating function while creating the absolute minimum amount of additional government structure. This approach is far more streamlined and efficient than other proposals, such as the creation of a separate cyber department or agency.

4. How would consolidating leadership for U.S. cybersecurity policy in a National Cyber Director provide greater direction for agencies as they implement the National Cybersecurity Strategy?

- The National Cyber Director would lead the coordination and integration of U.S. government defensive cyber activities, such as a federal government response to a significant cyber incident affecting the United States and "defensive cyber campaigns", or whole-of-government efforts designed to deter, defend against, mitigate, or limit the scope of an identified malicious cyber campaign. The National Cyber Director would act primarily as a convening authority in planning and coordinating these operations, ensuring that they are fully integrated, taking full advantage of participating department and agency authorities and capabilities, and reflecting the President's priorities. The NCD would also ensure appropriate coordination between defensive and offensive operations.
- Day-to-day execution of cybersecurity responsibilities would be carried-out by appropriate federal departments and agencies, such as CISA, the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), Sector Specific Agencies (SSAs), and others as appropriate.
- The National Cyber Director is not intended to override or interfere with the authorities and responsibilities of departments and agencies in their cyber missions, but to ensure that they are appropriately and effectively deconflicted, integrated, and mutually-supporting in their approaches, and receive necessary support in furtherance of broader government-wide efforts.
- The National Cyber Director should be granted sufficient latitude to coordinate operational responses, as necessary and appropriate, beyond the scope of previously established plans when required by evolving threats and exigent circumstances. The National Cyber Director should also carry out these responsibilities, to the greatest extent practicable, in coordination with the private sector and SLTT entities.

5. How would the National Cyber Director's proximity to the President, and connection to each Federal cybersecurity player, make a difference in our overall ability to manage cyber risks?

- The National Cyber Director would act as the President's principal advisor and spokesperson on cybersecurity and associated emerging technology issues and lead development of a National Cyber Strategy and associated policies that reflect national priorities; and ensure the implementation of the National Cyber Strategy across departments and agencies to include the effective integration of interagency efforts, and providing for the review of designated department and agency cybersecurity budgets. This can only be done effectively with the backing of the President.
- One of the executive branch's biggest obstacles to being effective in cyberspace has been consistency. Senior positions, and the experienced individuals who fill them, have come and gone within and across administrations, hampering strategic action. Creating

a Senate-confirmed position supported by an Office of the National Cyber Director in statute, like other organizations in the Executive Office of the President, will increase the coordination and accountability necessary to be successful in cyberspace. Requiring the National Cyber Director to be Senate confirmed will not only signal Congress' commitment to cyber issues, but also afford the Director a level of political support that bipartisan endorsement would bring.

6. Your testimony mentions that variability between different Administrations' approaches to cybersecurity leadership has "prevented the persistence and consistency needed to establish enduring policy and strategy."

a. Do you think creating the National Cyber Director position outlined in H.R. 7331 would help set the long-term vision needed for lasting progress on national policy goals?

- The National Cyber Director, and the Office of the NCD supporting them, will help bring strategic coherence to U.S. cyber policy. The Commission considered a number of models, and found the Office of the U.S. Trade Representative to be a good example of what is needed: a mission-oriented office, composed of subject matter experts coordinating government-wide strategy for an inherently interdisciplinary policy challenge.
- The prominence, and attendant influence, of the role of coordinating cyber issues has fluctuated across administrations, with some declining, at times, to fill the position at all. These changes have prevented the persistence and consistency needed to establish enduring policy and strategy. The Commission therefore determined the position and office would need a high level of prominence within the EOP to effectively coordinate national strategy and provide much needed leadership internationally, with SLTT organizations, and with the private sector.

b. Thinking several decades into the future, how could America's relationship with China and the rest of the world be altered by the establishment of a National Cyber Director?

Ensuring strong strategic leadership managing the risks in cyberspace will allow the United States to prosper and maintain its long-held standing in the world. To maintain leadership and superiority in cyberspace, artificial intelligence, and other technologies, the United States must maintain an edge and not only keep pace with technological change, but lead and drive innovation. The National Cyber Director can enable that long-term thinking, and ensure the support, planning, and capability-development necessary to execute the mission. Ultimately, the United States' ability to challenge its adversaries and support its allies and partners abroad must be built on a strong foundation at home; building that strong foundation requires the kind of strategic foresight and coordination that the National Cyber Director will enable.

QUESTIONS FOR THE RECORD

On behalf of Ranking Member James Comer (R-KY)

Committee on Oversight & Reform

Questions for Ms. Suzanne Spaulding:

1. Do our foreign allies have officials comparable to a National Cyber Director? If so, did the Commission study any of these foreign models?

Yes, the Commission studied, and even met with foreign officials, to discuss and learn from comparable foreign models for cybersecurity leadership. We engaged with the governments of the United Kingdom, Israel, Belgium, Estonia, and NATO as we designed our recommendations. The United Kingdom's success in establishing the Chief Executive Officer of the National Cyber Security Center was a guidepost for the Commission's recommendations on the National Cyber Director. The Estonian National Cyber Security Policy Director, as well as the Prime Minister's Cyber Security Advisor, and the Director of the Israeli National Cyber Security Authority, also served as examples of the need to elevate and empower cyber security within national leadership. Moreover, Israel's development of cybersecurity as an economic growth engine can be illustrative to the United States in how investment in cybersecurity can not only lead to better defended networks, but also spur growth and innovation.

The National Cyber Security Center in the UK and the structure of Estonian and Israeli cyber leadership helped to inform our belief in strong leadership at the highest level, with coordination of other agencies, and strong public-private coordination. In these discussions, the Commission recognized that the current structure, even with strengthened departments and agencies, still lacked institutionalized leadership, coordination, and a consistent advocate for the appropriate prioritization of cybersecurity as a national security issue. With this insight, the Commission deemed the institutionalization of a cyber coordinator position in the White House to be essential. To date, the existence of national cyber leadership has been a matter of executive branch policy. The prominence of the role has fluctuated across administrations, with some declining, at times, to fill the position at all. These changes have prevented the persistence and consistency needed to establish enduring policy and strategy. The Commission therefore determined the position and office would need a high level of prominence within the EOP to effectively coordinate national strategy and provide much needed leadership internationally, with SLTT organizations, and with the private sector.

2. In the "layered approach" to cybersecurity, one of the goals articulated by the Commission is to "deny benefits" to cyber enemies by securing "critical networks."

a. Did the Commission take a view on the potential use of Huawei and ZTE products in U.S. networks or networks operated by our allies like the U.K.? Should these companies' products be banned due to the risk posed by China?

The Commission argued that China uses cyberspace to accelerate its economic rise, undermine U.S. comparative strength, and suppress political opponents at home and abroad.[1] Chinese advanced persistent threat (APT) groups steal intellectual property and sensitive national security information. Beijing wages cyber-enabled economic warfare to fuel its rise while simultaneously undercutting U.S. economic and military superiority. Chinese cyber campaigns have enabled the theft of trillions of dollars in intellectual property. At the same time, Chinese APTs' aggressive cyber-enabled intelligence collection operations provide Chinese officials with improved intelligence information to use against the United States and its allies. Chinese operators constantly scan U.S. government and private-sector networks to identify vulnerabilities they can later exploit in a crisis. Targeting America's weapons and Defense Industrial Base enables Beijing to undermine opponents from within: for example, by threatening the U.S. Defense Industrial Base or driving a wedge between America and its allies. Taken to the extreme, China has the ability to launch cyberattacks in the United States that could cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline—for days to weeks.

Moreover, the Chinese Communist Party routinely harasses foreign and domestic dissidents in cyberspace while state-linked firms build a global mass-surveillance capability connecting information and communications equipment, surveillance cameras, facial recognition software, and massive data sets of private citizens. China is exporting these intrusive practices and technologies abroad, fueling a trend toward digital authoritarianism that threatens democracy at a global scale.[2] Chinese national companies like Huawei are part of an integrated strategy to use predatory pricing to dominate and eventually monop- olize key information and communications technology supply chains. The goal is to drive non-Chinese alternatives out of business, leaving the Chinese Communist Party and its business allies with a stranglehold on the global supply chain. As China exports this equipment, it becomes the central hub of a new network of authoritarian states that use mass surveillance and technologies of control, such as social credit, to suppress fundamental human rights. Empowering China's intelligence collection apparatus is its National Intelligence Law which requires companies operating in China to cooperate with and turn over to the Chinese government any requested data. This law essentially turns Chinese telecommunications firms into Chinese espionage firms. Unchecked, Chinese economic warfare, espionage, and repression of civil liberties are likely to continue.

---

[1] Wayne M. Morrison, "The Made in China 2025 Initiative: Economic Implications for the United States," (Congressional Research Service, April 12, 2019, https://fas.org/sgp/crs/row/IF10964.pdf.

[2] For an overview of cyber operations attributed to China along these lines, see Citizen Lab reporting: https://citizenlab.ca/tag/china/.

Without a new whole-of-nation strategy and significant changes to how the United States defends its networks in cyberspace, Chinese operations will continue to threaten long-term American economic prosperity and national security. Revelations of high-profile security failures of information will undermine confidence in the U.S. government's ability to protect its citizens and businesses. Along with the loss in national power, trust in American institutions will wither. In the minds of regional allies, perceptions of unchallenged Chinese operations will reduce the credibility of American security guarantees. Exfiltration of private-sector intellectual property could compel investors to question the viability of the U.S. economy as a hub of technological innovation. Breaches could also yield intelligence coups that threaten the United States' clandestine personnel and advance Beijing's diplomatic and economic goals. Stolen U.S. military technology will enable the production of capable facsimiles and support the design of People's Liberation Army weapon systems that exploit newly identified vulnerabilities in U.S. counterparts. Compromised supply chains could undermine American military operations in future wars.[3] China is seeking to monopolize how people around the world interact, pay for goods, and relate to their governments. As Chinese- built networks and applications mediate interactions, Beijing gains unprecedented power to surveil and control the lives of individuals worldwide. Civil liberties and open markets will struggle to survive in this new era of cyber repression. China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the U.S. government, corporations, and allies. It is improving its cyberattack capabilities and altering information online, shaping Chinese views and potentially the views of U.S. citizens.[4]

While the Commission did not specifically focus on the question of whether to ban Chinese products, it does argue that the implementation of its recommendations will create a stronger and more resilient cyberspace where Chinese attacks will be either prevented, or rendered less effective. We must also acknowledge the importance of working with allies and partners. The challenge posed by Huawei and ZTE highlights that we alone as a nation cannot address these threats and need to do a better job of getting our allies and partners on board with collective efforts.

b. What infrastructure networks in our country are most at risk and what entities own and operate these entities? Water, electric, healthcare, banking and financial services, transportation, etc.?

The Commission has made the argument that there is a wide disparity between the haves and have nots in terms of cybersecurity in infrastructure networks. Some, like the financial services

[3] Justin Sherman and Robert Morgus, "Authoritarians Are Exporting Surveillance Tech, and with It Their Vision for the Internet," Council on Foreign Relations, December 5, 2018,https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet.

[4] Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community" (Office of the Director of National Intelligence, January 29, 2019), 5, 7, https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.29

and energy sectors, have strong SSAs and robust sharing and coordination mechanisms capable of defending their networks from daily cyberattacks, paired with large investments in cybersecurity. Water systems, on the other hand, are among the most vulnerable of our nation's critical infrastructure. Every American, every day, depends on a supply of clean water. Yet most Americans would be surprised to learn that even though water is critical in our daily lives, and even though our water supply is known to be a target for malign actors, water utilities remain largely ill-prepared to defend their networks from cyber-enabled disruption.[5]

The U.S. water supply is operated by nearly 70,000 utilities[6] that are turning to digital networks to manage real-world physical processes critical to water treatment and distribution—but these utilities are approaching this transition with dramatic variations in capacity and sophistication. Like our electoral system, this distributed network can provide a measure of resilience. Also like our electoral system, it can limit the effectiveness of federal action and slow the deployment of best practices or the responsible incorporation of secure technologies. Gaps in utilities' network configurations, insecure remote access systems, and outdated training regimes are just a few of the vectors through which Americans' water infrastructure is vulnerable to cyber-enabled exploitation.[7] Malign actors have already attempted to breach water infrastructure systems, and they could eventually exploit these vulnerabilities to disrupt or contaminate the American water supply.[8]

Compounding these problems, municipal utilities often lack the resources or capacity to address these weaknesses. In partnership with the Department of Homeland Security, federal sector-specific agencies (SSAs) and state and local governments are currently responsible for managing and securing American utilities. For the water sector, the Environmental Protection Agency (EPA) is the principal federal agency responsible for cyber risk management.[9] In practice, however, SSA responsibilities are unclear, and that uncertainty contributes to insufficient coordination between the EPA and other stakeholders in water utilities' security, as well as to cybersecurity funding requests that lack the resources and buy-in necessary for success.

These shortcomings imperil the cybersecurity of our water infrastructure, which is vital to our

---

[5] For cyber risk posed by malign actors to water infrastructure that is known by water utility companies, see Judith H. Germano, "Cybersecurity Risk & Responsibility in the Water Sector" (American Water Works Association, 2019), 7–9, https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319- 13. For current network defense limitations of water utilities, see Robert M. Clark, Srinivas Panguluri, Trent D. Nelson, and Richard P. Wyman, "Protecting drinking water utilities from cyberthreats" (Idaho National Labs, February 2, 2017), 13–15, https://www.osti.gov/servlets/purl/1372266.

[6] Blake Sobczak, "Hackers Force Water Utilities to Sink or Swim," E&E News, March 28, 2019, https://www.eenews.net/stories/1060131769.

[7] Clark, Srinivas, Nelson, and Wyman, "Protecting Drinking Water Utilities from Cyberthreats," 13–15.

[8] For attempted breaches by Russia: "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A. For attempted breaches by others: Germano, "Cybersecurity Risk & Responsibility in the Water Sector," 7–9.

[9] See "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, December 17, 2003, https://www.cisa.gov/homeland-security-presidential-directive-7.

lives. Codifying SSA responsibilities, ensuring that SSAs such as the EPA conduct their risk management assignments effectively, and better enabling state and local governments are all critical steps toward improving the capacity of water utilities to prevent and mitigate the growing threats they face from cyberspace.

c. In terms of our energy networks, some often cite cyber risk for choosing not to build new nuclear plants. Has a country like France, which operates a significant nuclear infrastructure, faced significant cyber-attacks on its nuclear plants? Did the Commission study cyber risk to potential alternative energy sources?

While the Commission did not specifically study cyber risk to potential alternative energy sources, our holistic look at the critical infrastructure of the United States gleaned important insights that are as relevant to nuclear plants as to other energy utilities. Due to the persistent work of the Department of Energy and the U.S. Nuclear Regulatory Commission to safeguard nuclear energy in cyberspace, the U.S. energy sector is one of the stronger critical infrastructure sectors in terms of cybersecurity.

Nuclear plants, like other energy utilities have become more vulnerable to cyber attacks in recent years as operational systems have gone increasingly online. In 2018, for example, hackers obtained the plans for France's nuclear power plants in a cyber attack. As these threats grow, it is imperative that the U.S. continue to protect all energy critical infrastructure, not just nuclear power, as they are all vulnerable to cyber attacks.

3. It is often said that the security of networks is only as safe as the conduct of individuals on those networks. Phishing scams continue to be a primary vector of attack. Did the Solarium Commission study this weakness? Any recommendations?

The Commission did review the security of networks as a byproduct, and the conduct, of the users of those networks. While we ultimately focused our recommendations on the organizations and critical infrastructure owners and operators that could make some of the largest organizational changes to improve *overall* cybersecurity, the Commission strongly supports public education on cyber hygiene and other user-focused security efforts. The Commission recommended the need for greater promotion of good cyber hygiene practices among both companies and the general public to stop malicious actors from succeeding in carrying out phishing and other means of intrusion. Use of multi-factor authentication, or a system that requires a password and an additional method, such as a text or an "authenticator" application, for users to authenticate their identity when logging into a system, is a prime example. A Google study showed that it can prevent roughly 96 percent of bulk phishing attacks and more than three-quarters of targeted attacks.[10]

[10] Kurt Thomas and Angelika Moscicki, "New Research: How Effective Is Basic Account Hygiene at Preventing Hacking," Google Blog, May 17, 2019, https://security.googleblog.com/2019/05/new-res earch-how-effective-is-basic.html.

Next, the Commission recommends Congress pass a national data security and privacy protection law establishing and standardizing requirements for the collection, retention, and storage of user data. The Commission also recommends Congress should establish and fund a National Cybersecurity Certification and Labeling Authority empowered to establish and manage a program for voluntary security certifications and labeling of information and communications technology products. The lack of differentiation in products leads to a lack of demand for more secure products; as a result, product developers have little market incentive to make established security standards or security best practices a primary consideration in designing, testing, and developing their products. With clearer labelling, users can be better informed, and therefore better protected. The U.S. government should also promote digital literacy, civics education, and public awareness to build societal resilience to foreign, malign cyber-enabled information operations.

4. The Commission said that we must "impose costs" on our adversaries who choose to attack us through cyber means. U.S. Cyber Command is organized to go on the offense. Other entities in the Intelligence Community (IC) also have that power.

The strategy put forth by the Commission, "**layered cyber deterrence**", combines a number of traditional deterrence mechanisms and extends their use beyond the government to develop a whole-of-nation approach. It also updates and strengthens our declaratory policy for cyberattacks both above and below the level of armed attack. The United States must demonstrate its ability to impose costs while establishing a clear declaratory policy that signals to rival states and nonstate actors the costs and risks associated with attacking America in cyberspace. The Cyber Mission Force (CMF) is where the bulk of the capabilities exist within the DoD to counter malicious adversary campaigns and impose costs Additionally, while U.S. Cyber Command is organized for offensive cyber missions, it also has an equally--and, in some cases, more--important defensive mission and it maintains teams that are organized for defense. The Commission has emphasized the important links between offense and defense in cyberspace.

The Commission acknowledges that entities beyond the Department of Defense/U.S. Cyber Command have unique capabilities and authority to impose costs on adversaries in cyberspace. This includes organizations and agencies within the Intelligence Community. The Commission has emphasized that cost imposition in cyberspace should entail the holistic and integrated application of various instruments of national power.

a. Could you describe the instances where you would recommend Cyber Command responding in retaliation with offensive measures?

The Commission refrained from providing specific recommendations as to the conditions under which U.S. Cyber Command, or any other entity, should retaliate against malicious adversary cyber behavior with offensive measures. This should be a function of the particular circumstances of the situation. Additionally, Congress made significant strides in addressing this issue in the fiscal year 2019 National Defense Authorization Act, specifically in Section 1642.

To further improve on Congressional action in the 2019 NDAA, the Commission did recommend **reviewing the delegation of DoD authorities** to ensure that they are sufficiently delegated down to enable more rapid decision-making to conduct cyber campaigns. This would, among other things, improve processes to enable retaliation with offensive measures with warranted, appropriate, and authorized.

b. Imposing costs seems to be a concept that could cause reciprocation. What are the risks?

The Commission's recommendations on defense and resilience are meant, in part, to address potential concerns about retaliation. By enhancing our domestic resilience, while also imposing costs, we make it harder for our adversaries to respond in a significant way. Specifically, the Commission argues:

- Defending forward, in addition to leveraging other instruments of power, frustrates our adversaries' ability to act with impunity.
- Furthermore, the very act of conducting defend forward cyber operations helps to identify adversary organizations, reveal their attack infrastructure, illuminate their capabilities, tactics, tradecraft, and personas, and fundamentally aids in attribution as well as the defense of the United States and our allies and partners. It does so by exposing these actors and their tradecraft to network defenders.
- The very dynamism and volatility of cyberspace that you correctly noted make it even more imperative for the United States to be proactive, rather than reactive, to maneuver where adversaries operate, to collect against their capabilities and organizations, and to thwart their operations when appropriate to stay one step ahead of these threat actors.
- Related to discussions of laws and norms, the United States has long maintained a more flexible stance on the distinction between "use of force" and "armed attack." More specifically, the U.S. asserts that any unlawful use of force can qualify as an armed attack, triggering the right of self-defense.
- Few, if any, cyber operations have actually crossed the armed attack threshold. Indeed, the crux of the policy challenge for the United States is how to address malicious adversary campaigns that may not even rise to the level of "use of force" but that nevertheless have strategic implications.
- Across all domains, the specific definition of *what actions* would constitute a use of force or rise to the level of armed conflict remains an inherently political decision. This should continue to be the case in cyberspace as well. The United States can and must clearly signal the kinds of unacceptable activities that would trigger such thresholds, but without constraining the ability of political leadership to maneuver and adapt in the midst of a crisis.
- Our Commission was also clear that the nuclear age is fundamentally different from the cyber one and, therefore, key strategic concepts need to be updated to take into account the particular challenges posed by the cyber domain.

c. Is the intelligence community properly organized to impose costs on adversaries for cyber-attacks?

Yes. The Title 50 system is working and has been given more clarity of purpose with the recent creation of the NSA Cybersecurity Directorate which will redefine the NSA cybersecurity mission and enhance its partnerships with unclassified collaboration and information sharing.

To support this critical investment, the Commission has a number of recommendations, including: strengthening CTIIC to ensure its ability to carry out its responsibilities, especially in enhancing the quality and speed of attribution; updating PDD-41 to achieve clear incident response protocols and command and control; and improved information sharing and intelligence prioritization with the private sector. The Commission also recommends that Congress direct the Department of Defense to conduct a force structure assessment of the Cyber Mission Force, given increases in adversary activity over time and an expanded mission set. As part of that assessment, the Commission recommends an assessment of the resource implications for the organizations within the intelligence community in their combat support agency role.

d. Does the intelligence community need any further authorities in order to implement a strategy of imposing costs for malevolent activity by our adversaries?

While the intelligence community was consulted during the extensive Commission engagements with federal agencies, neither the intelligence community nor CYBERCOM requested new authorities. The inclusion of cyber surveillance and reconnaissance in the FY19 NDAA, coupled with NPSM 13 and existing Title 50 authorities, are sufficient for the implementation of a cost imposition strategy. The Commission does, however, recommend the authority to review delegations to NSA should include those authorities that enable the agency to rapidly tip relevant foreign intelligence collection to private entities that constitute the Defense Industrial Base and their service providers to support the latter's own defensive operations.

e. What authorities would the Cyber Director have over intelligence community and Defense Department led offensive and incident response activities? Would the NCD office be a peer coordinating entity or would it have any actual ability to influence the activities of the nation’s intelligence and defense functions?

The National Cyber Director’s scope of authority for planning and coordination should be limited to tactical or strategically defensive cyber operations and activities conducted in defense of the homeland, and exclude intelligence and offensive operations conducted daily pursuant to collection requirements and warfighting plans. However, the intelligence community agencies and the Department of Defense do undertake defensive cyber activities for the homeland and contribute significantly to whole-of-government cyber efforts to defend the homeland.

It is the Commission's recommendation that such activities undertaken by these agencies, to include counter-cyber operations, be included in the National Cyber Director's scope of responsibility for planning and coordination of defensive cyber campaigns.

5. Through the Commission's recommended policy of "shaping behavior" - enforcing norms of responsible cyber behavior – how do diplomacy, sanctions, and even indictments deter malicious actors?

Cyber deterrence is not nuclear deterrence. The fact is, no action will stop every hack. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly to successfully attack American interests through cyberspace. Layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries (e.g., denial and cost imposition) with forms of influence optimized for a connected era, including strengthening norms for responsible behavior in cyberspace. Enforcing norms through credible enforcement of costs, such as sanctions, and indictments is key to detering malign behavior. This deterrence is even more impactful when performed in concert with partners and allies, which highlights the importance of diplomacy in this area. When bad-actors know that they will be met with collective punishment for rule-breaking their decision calculus is altered.

a. Have you seen evidence of the success of these actions in deterring malicious behavior?

The point of deterring malicious behavior though credible costs is to prevent attacks. When the United States is successful at deterrence, the ultimate result will be a reduction of malign actions towards the U.S. and our partners and allies. Without a clear baseline and consistent longitudinal data, tracking and measuring this reduction is impossible. Accordingly, to see deterrence at work—that is to detect that attacks *are not* happening when they otherwise might have—we need better metrics on activity in cyberspace. This is part of the reason why the Commission recommends the creation of a Bureau of Cyber Statistics to collect and develop statistical data on these trends and other relevant information that will allow the United States to better gauge progress. Where we do see success is in the deterrence of malicious behavior during the 2018 election cycle. In increasing effectiveness with which the United States engages with other countries to impose costs, we can build a team of allies which can work together to prevent adversary action. A prime example is the Department of State's Cyber Deterrence Initiative, which has begun work with allies and partners to increase the speed at which attribution, and subsequent cost imposition, can be made.