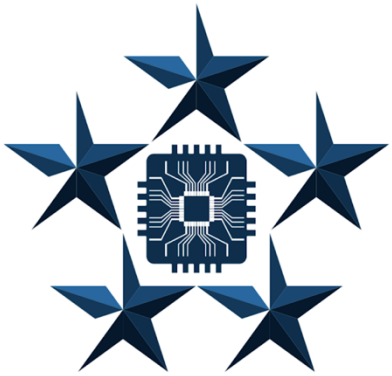

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

Testimony of:

Senator Angus King,
Representative Mike Gallagher,
Ms. Suzanne Spaulding, and
Mr. Tom Fanning

Commissioners of the
Cyberspace Solarium Commission

Before the United States Senate Committee on Homeland Security and Governmental Affairs

"Report of the Cyberspace Solarium Commission"

May 13, 2020

INTRODUCTION - INTENT OF THE COMMISSION

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The Commission consists of fourteen Commissioners, including four serving legislators, four executive branch leaders, and six recognized experts with backgrounds in industry, academia, and government service. Senator Angus King and Representative Mike Gallagher serve as Co-Chairmen. The Commissioners spent the past eleven months studying the issue, investigating solutions, and deliberating courses of action to produce a comprehensive report. As a group we met 29 times in weekly meetings and the staff conducted nearly 400 interviews with industry, federal, state and local governments, academia, non-governmental organizations, and international partners. We then stressed tested our findings and red teamed different policy options in an effort to distill the optimal approach.

The Commission developed a strategic approach of layered cyber deterrence and identified 82 specific policy or legislative remedies. The legislative recommendations were subsequently turned into 57 legislative proposals that have been shared with the appropriate Senate and House committees. The final report was presented to the public on March 11, 2020.

Throughout this process the Commission always considered the Congress as its “customer.” Through the NDAA, the Congress tasked the Commission to investigate the issue of cyber threats that undermine American power and to determine an appropriate strategic approach to protect the nation in cyberspace and identify policy and legislative solutions to achieve that objective. We four Commissioners are here today to tell you what we learned, advocate for our recommendations, and work with you to assist in any way we can to solve this complex challenge.

FOCUS OF OUR EFFORT

Cyber defense and resilience of the nation form the foundation of the Commission’s strategy. Critical infrastructure - the systems, assets, and entities that underpin our national and economic security, and public health and safety - are increasingly threatened by malicious cyber actors. Effective critical infrastructure security and resilience require a clear and consistent declaratory policy backed up with the credible threat to impose costs to deter adversaries from targeting the nation in the first place. This also requires reducing the consequences of adversary disruption of critical infrastructure, minimizing its vulnerabilities, and thwarting adversary operations that seek to hold critical infrastructure at risk.

First and foremost, Congress should establish a National Cyber Director within the Executive Office of the President to centralize and coordinate the cybersecurity mission at the national

level. The National Cyber Director will work among Federal departments and agencies to bring coherence both to the development of cybersecurity policy and strategy as well as its execution. This Senate confirmed position will provide clear leadership in the White House and signal cybersecurity is an enduring priority in U.S. national security strategy.

Additionally, a key element of a coherent and consistent cyber strategy across the U.S. government is a clearly articulated deterrence posture, buttressed by a strong declaratory and signaling policy that the U.S. will swiftly respond to impose costs against adversaries who seek to use cyberspace to undermine our interests and values and attack us where we are asymmetrically vulnerable. This declaratory policy should span the range of malicious adversary behavior, including cyberattacks above the use of force threshold as well as adversary campaigns that occur below the level of war. To be credible, we must back up our statements with consistent (and, where possible, transparent) action if and when our adversaries test us.

Second, the government should continue to improve the resourcing, authorities and organization of the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience. The Commission recommends empowering CISA with greater tools to strengthen public-private partnership, including a Joint Collaborative Environment for real-time information exchange and analysis; an Integrated Cyber Center for person-to-person collaboration; and a Joint Cyber Planning Cell for public-private planning that can be rapidly actioned in a crisis. These changes will forge the public-private collaboration necessary to quickly detect, mitigate, and respond and recover from a significant cyber incident.

Third, the United States should take immediate steps to strengthen the resilience of our critical infrastructure. Reducing the consequences of a cyberattack is critical for denying benefits that our adversaries can expect from their operations. These include disruption, intellectual property theft, and espionage. The Commission recommends that Congress codify Sector-Specific Agencies as Sector Risk Management Agencies and strengthens their ability to aid critical infrastructure sectors in identifying and managing the risks they face. This work will be critical to establish a Continuity of the Economy Plan: government-wide and public-private contingency planning to rapidly restart the U.S. economy after a major disruption. In addition, the Commission recommends establishing a Cyber State of Distress tied to a Cyber Response and Recovery Fund. This would give the government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical national functions can continue to operate during a sustained disruption or crisis.

Finally, the Commission recommends two relevant initiatives to reshape the cyber ecosystem and reduce vulnerabilities. The first, the creation of a National Cybersecurity Certification and Labeling Authority, will establish standards and transparency to allow consumers of technology products and services to demand more security and less vulnerability in the technologies they purchase. The second, forming a Bureau of Cyber Statistics, will create better information to

improve the security behavior of individuals and organizations. A Bureau of Cyber Statistics will provide private companies, the public, and government policymakers with an empirical evaluation of what does and does not work in cybersecurity. It will also publish cybersecurity data to inform public policy and cybersecurity investments in the public and private sectors.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID-19 pandemic has been a learning experience for us as it illustrates the challenge of ensuring resilience and continuity in a connected world. It is an example of a type of crisis that spreads rapidly through a system, stressing everything from emergency services and supply chains to basic human needs. The pandemic produces cascading effects and high levels of uncertainty. This situation undermines normal policy-making processes and forces decision makers to craft hasty and ad hoc emergency responses. The Commission evaluated exactly this type of event--complex emergencies that rely on coordinated action beyond traditional agency responses--so that the U.S. does not get caught unprepared by a massive cyberattack.

The lessons the country is learning from the ongoing pandemic are not perfectly analogous to a significant cyberattack, but some parallels are obvious. First, the pandemic and a significant cyberattack are global in nature. Second, both require a whole-of-nation response effort and are likely to challenge existing incident management doctrine and coordination mechanisms. Finally, and perhaps most importantly, prevention is usually far cheaper and more effective than response.

The global health crisis has reinforced the urgency of many of the core recommendations in the Commission's March 2020 report. Responding to complex emergencies will require a balance between response agility and institutional resilience in the economy and critical infrastructure sectors. It relies on strategic leadership and coordination from the highest offices in government, underscoring the importance of a National Cyber Director. It also demands a strong understanding of the risks posed by a crisis and a data-driven approach to mitigating them before, during, and after it, validating the Commission's recommendation to codify Sector-specific Agencies, create a Bureau of Cyber Statistics, and establish a National Risk Management Cycle. Agility in responding to a crisis rests on clear roles and responsibilities for critical actors in the public and private sectors as well as established, exercised relationships and plans, highlighting the importance of Continuity of the Economy planning. The imperative of social distancing during the crisis has brought renewed urgency to securely digitize critical services, stressing the importance of the Commission's recommendation to incentivize the movement to the cloud and broader modernization in state, local, tribal, and territorial governments.

THE CHALLENGE

The more connected and prosperous our society becomes, the more vulnerable we are to nation-state rivals, rogue states, extremists, and criminals. As a result, for the last twenty years, adversaries have used cyberspace to attack American power and interests, and our lack of

response has taught them that, if they attack us in cyberspace, they will not pay a price. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the U.S. government, the private sector, and the public at large.

The American public relies on critical infrastructure, 85% of which, according to the U.S. Chamber of Commerce, is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment to hospitals—are connected and vulnerable. Furthermore, new industries and services, such as cloud computing, have become increasingly important economic growth. As we saw last year, malicious cyber actors don't just target the U.S. government and military personnel--they increasingly target our cities and counties with malware and ransomware attacks.

Creating a secure nation in the 21st century requires an interwoven system of both public and private networks defended from state and non-state threats.

China 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.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In the spring of 2014, Russian-linked groups launched a campaign to interfere in Ukrainian elections that included attempts to alter voter tallies, disrupting election results through distributed-denial-of-service attacks, and smearing candidates by releasing hacked emails. During the 2016 U.S. presidential campaign, Russian operatives used cyber operations to collect and release damaging information on political parties and candidates and conduct influence operations using social media. Since 2016, Russia has continued to spread hate and disinformation on social media to polarize free societies and seek to interfere in democratic elections. But Russia has not stopped there. The 2017 NotPetya malware attack, attributed to Russia, spread around the world and temporarily shut down major international businesses and affected critical infrastructure. Russian-affiliated groups have even gained access via cyberspace to surveil nuclear power plants in the United States.

Iran and North Korea also use cyberspace to attack U.S. and allied interests. Iranian cyber operations have targeted the energy industry, entertainment sector, and financial institutions. Iranian-affiliated threat actors have also targeted dams in the United States with distributed-denial-of-service attacks. North Korea exploits global connectivity to skirt sanctions and sustain an isolated, corrupt regime. According to UN estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year. The 2017 WannaCry ransomware attack, attributed to North Korea, impacted over 300,000 computers in 150 countries, including temporarily disrupting UK hospitals.

Finally, a new class of criminals thrives in this environment. Taking advantage of widespread cyber capabilities revealed by major state intrusions, criminal groups are migrating toward a "crime-as-a-service" model in which threat groups purchase and exchange malicious code on the dark web. In 2019, ransomware incidents grew over 300% compared to 2018 and affected more than 40 U.S. municipalities. More recently, opportunistic hackers have hijacked hospitals and healthcare systems during the COVID-19 pandemic, taking advantage of poorly protected systems in their most vulnerable states. As the world changes to meet the needs of a global pandemic, remote access and the growth in the work-from-home economy continue to increase the threat vectors for criminal actors.

STRATEGIC APPROACH

In the face of this challenge, the Commission understands that to secure America in the 21st century requires securing cyberspace. To accomplish that end, the Commission proposes a new approach: layered cyber deterrence. This strategy combines a number of traditional deterrence mechanisms and extends them 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 the costs and risks associated with attacking us in cyberspace.

Since America relies on critical infrastructure that is primarily owned and operated by the private sector, the government cannot defend the nation alone. The public and private sectors, along with key international partners, must collaborate to build national resilience and reshape the cyber ecosystem to increase its security, while imposing costs against malicious actors and preventing attacks of significant consequence.

The Commission acknowledges that, while deterrence is possible in cyberspace, it is not the same as nuclear deterrence. Successful nuclear deterrence was defined as the absence of any use of nuclear weapons. However, in cyberspace, the reality is that no action will stop every operation. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly for malicious actors to benefit from targeting American interests through cyberspace. Therefore, layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries, such as denial and cost imposition, with forms of influence optimized for a connected era, such as promoting norms that encourage restraint and incentivize responsible behavior in cyberspace. Strategic discussions all too often prioritize narrow definitions of deterrence that fail to consider how technology is changing society. In a connected world, those states that harness the power of cooperative, networked relationships gain a position of advantage over other states. However, vulnerabilities that come with this connectivity means that leading states, such as the United States, need to arrive at shared understandings about what constitutes acceptable behavior in cyberspace. It also requires shaping adversary behavior by changing the ecosystem in which competition occurs, not only threatening to impose costs. Finally, it demands international engagement and collaboration with the private sector.

Layered cyber deterrence emphasizes working with the private sector to efficiently coordinate how the nation responds with speed and agility to emerging threats. The federal government alone cannot fund or solve the challenge of adversaries attacking or exploiting the networks on which America and its allies and partners rely. The federal government must collaborate with state and local authorities, leading business sectors, and international partners, within the rule of law. Layered cyber deterrence also addresses the planning needed to ensure continuity of the economy and the ability of the United States to rebound in the aftermath of a major, nationwide cyberattack of significant consequences. Such planning adds depth to deterrence by assuring the American people and our allies, and conveying to our adversaries that the United States has the will and capability to respond to any attack on its interests.

The implementation of layered cyber deterrence is organized around 6 different pillars, each of which focuses on one aspect of the strategy.

THE NEED TO REORGANIZE THE U.S. GOVERNMENT (PILLAR 1)

To defend U.S. interests in cyberspace, key government authorities and processes must be adjusted and aligned. This requires that the Legislative and Executive Branches better align their authorities and capabilities; the public and private sectors improve collaboration in the defense of critical infrastructure and integration in the planning, resourcing, and employment of government cyber resources; and strategic continuity and unity of effort across the U.S. government.

First, Congress must reestablish clear oversight responsibility and authority over cyberspace within the Legislative Branch. The large number of committees and subcommittees claiming some form of jurisdiction over cybersecurity matters is actively impeding action and clarity of oversight. By centralizing responsibility in the new House Permanent Select and Senate Select Committees on Cybersecurity, Congress will be empowered to provide coherent oversight to government strategy and activity in cyberspace.

Next, select entities in the Executive Branch that address cybersecurity must be restructured and streamlined. Multiple departments and agencies have a wide range of responsibilities for securing cyberspace. These responsibilities tend to overlap and at times conflict. Executive Branch departments and agencies tend to compete for resources and authorities, resulting in conflicting efforts that produce diminishing marginal returns. Establishing a Senate confirmed National Cyber Director within the Executive Office of the President would consolidate accountability for harmonizing the Executive Branch's policies, budgets, and responsibilities in cyberspace while implementing strategic guidance from the President and Congress.

In addition to the National Cyber Director, properly resourcing and empowering CISA is critical to achieving coherence in the planning and deployment of government cyber resources. Multiple administrations and Congressional sessions have worked to establish CISA as a keystone of national cybersecurity efforts. However, work remains to be done to realize the Commission's ambitious vision for this critical organization. This includes strengthening CISA's director with a five-year term and elevated executive status, adequately resourcing its programs to engage with

the private sector while managing national risk, and securing sufficient facilities and required authorities for its vital and growing mission. These changes will remove key limitations in CISA's ability to forge a greater public-private partnership and its mission to secure critical infrastructure.

Finally, the U.S. government must more effectively recruit, develop, and retain a cyber workforce capable of building a defensible digital ecosystem and deploying all instruments of national power in cyberspace. This requires designing innovative programs and partnerships to develop the workforce, supporting and expanding current high-performing programs, and connecting with a diverse pool of promising talent. Successfully building a robust federal workforce, in some cases, may depend on stakeholders outside the federal government, such as educators, non-profits, and businesses. Policymakers should support these important partners by providing the tools they need to be effective, such as classroom-ready resources, incentives for research on workforce dynamics, and clear routes for collaborating with the government.

DETERRENCE BY DENIAL (PILLARS 3/4/5)

Denying adversaries the benefits of their cyber campaigns is a critical aspect of layered cyber deterrence. Denial comprises ensuring the resilience of critical pillars of national power, reducing our national vulnerability, and disrupting threats through operationalizing collaboration between the government and private sector. Together, these actions can effectively force adversaries to make difficult decisions regarding resourcing and carrying out malicious cyber operations and campaigns.

Denying benefits to adversaries starts with ensuring that our most critical targets are able to withstand and quickly recover from cyberattacks. In other words, we must build resilience. Effective national resilience efforts fundamentally depend on the ability of the United States to accurately understand, assess, and manage national cyber risk. Current efforts to do so at the national level are relatively new and are significantly hindered by resource limitations, immaturity of processes, and inconsistent capacity across the departments and agencies that participate in national resilience efforts.

Today, under the direction of Presidential Policy Directive 21, sector-specific agencies are the lead federal agencies tasked with day-to-day engagement with the private sector on cybersecurity and resilience. However, there are significant imbalances and inconsistencies in both the capacity and the willingness of these agencies to manage sector-specific risks and participate in government-wide efforts. In addition, the lack of clarity and consistency concerning the responsibilities and requirements for these agencies continues to cause confusion, redundancy, and gaps in resilience efforts. For this reason, the Commission recommends codifying sector-specific agencies in law as "Sector Risk Management Agencies," establishing baseline responsibilities and requirements for managing risk in the sector or sectors under their purview, and appropriating necessary funds to carry out their responsibilities. In addition, the

Commission recommends that Congress recognize, in law, the lead role of the CISA in national risk management.

With more robust risk management capability in the federal government, Congress must also codify the process whereby these agencies come together to provide the federal government with a clearer picture of where we are vulnerable and where we need to place greater resources. The U.S. government has made great strides at understanding national risk through DHS's national critical functions work. However, the U.S. government lacks a rigorous process for identifying, assessing, prioritizing, and ultimately buying down national risk to critical infrastructure. To fill this gap, the Commission recommends that Congress codify a five-year "national risk management cycle" in law to culminate with a "Critical Infrastructure Resilience Strategy" and an accompanying "National Cybersecurity Assistance Fund" to ensure consistent funding for initiatives that underpin or build resilience.

National resilience similarly requires sufficient national capacity and preparedness to respond to and recover from attacks when they do happen. The United States has well-established mechanisms and processes to respond to physical and natural disasters and states of emergency. However, the U.S. government has not yet applied the same rigor to understanding and responding to cyber states of distress and disasters. To address this shortcoming, the Commission recommends Congress pass a law codifying a Cyber State of Distress and an accompanying Cyber Response and Recovery Fund to assist state, local, tribal, and territorial (SLTT) governments and the private sector beyond what is available through conventional government technical assistance and cyber incident response programs.

Similarly, while Continuity of Operations and Continuity of Government have long been cornerstones of government contingency planning, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major disruption. That is why the Commission recommends that Congress direct the Executive Branch to develop and maintain Continuity of the Economy planning to ensure continuous operation of critical functions of the economy in the event of a significant cyber disruption. The planning process should analyze national critical functions, outline priorities for response and recovery, and identify areas for resilience investments. In doing so, the Continuity of the Economy plan should identify areas for preservation of data and mechanisms for extending short-term credit to ensure recovery efforts.

Beyond ensuring resilience, a second major aspect of denying benefits to adversaries lies in reducing our national vulnerability at scale. Today, vulnerabilities in our cyber ecosystem not only derive from technology, but also from human behavior and processes. The Commission sought to improve the security of both the technological and human aspects at scale. Moving the technology markets to emphasize security requires increasing transparency about the security characteristics of consumer technology products. Therefore, the Commission recommends creating a National Cybersecurity Certification and Labeling Authority to develop and facilitate authoritative, easy to understand security certifications and labels for technology products.

Driving down vulnerability in human behavior and processes requires a combination of better empirics to understand what constitutes good cybersecurity behavior and incentives to nudge humans and organizations toward that better behavior. To address the former, the Commission recommends the creation of the Bureau of Cyber Statistics, which will gather relevant data, analyze it, and publish insights for policymakers and the public.

Armed with better information about best practices in cybersecurity, policymakers must find a mixture of incentives to encourage individuals and organizations to adhere to them. Insurance is one such incentive. Although the insurance industry plays an important role in enabling organizations to transfer a small portion of their cyber risk, it is falling short of achieving the public policy objective of driving better practices of risk management in the private sector more generally. Because insurance falls under the purview of state regulators, the federal government can do little to directly affect change in the market for insurance specific to a given industry. Thus, to improve the market for cybersecurity insurance, Congress should appropriate funds and direct DHS to resource a Federally Funded Research and Development Center to develop models for underwriter and claims adjuster training and certification and establish a public-private partnership on modeling cyber risk.

The final aspect of denying adversaries benefits lies in disrupting their operations. Cyber defense, while a shared responsibility, will significantly depend on the underlying efforts of the owners and operators of private networks and infrastructure. The U.S. government and industry thus must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This “collective defense” in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense. Therefore, the Commission recommends codifying the “systemically important critical infrastructure” designation for entities responsible for systems and assets that underpin national critical functions. This will hold these entities to a higher standard and ensure they are fully supported by the U.S. government. Additionally, U.S. government support must be better informed through a Joint Collaborative Environment that would pool public-private sources of threat information to be coordinated through a Joint Cyber Planning Cell and an Integrated Cyber Center at DHS.

DETERRENCE BY SHAPING BEHAVIOR (PILLAR 2)

Layered cyber deterrence includes shaping cyber actors’ behavior through strengthening norms of responsible state behavior and employing non-military instruments of power, such as law enforcement, sanctions, diplomatic engagement, and capacity building. A system of norms, based on international engagement and enforced through these instruments of power, helps secure American interests in cyberspace.

To strengthen cyber norms and build a likeminded international coalition to enforce them, the Commission recommends Congress create and adequately resource the Bureau of Cyberspace Security and Emerging Technologies led by an Assistant Secretary of State. The Bureau will bring dedicated cyber leadership and coordination to the Department of State.

Leading internationally also means having strong and coordinated representation in bodies that set global technical standards. Therefore, the Commission recommends that Congress should sufficiently resource the National Institute of Standards and Technology to bolster participation in these bodies. American values, interests, and security are strengthened when international technical standards are developed and set with active U.S. participation. The U.S. must also facilitate robust and integrated participation from across the federal government, academia, civil society, and industry. The U.S. is at its best when we draw input from *all* our experts.

In parallel to robust participation in multilateral bodies, law enforcement activities also provide fruitful ground on which to work with international partners and allies to hold adversaries accountable for malicious behavior. The Commission recommends providing the Department of Justice Office of International Affairs with administrative subpoena authority that streamlines the Mutual Legal Assistance Treaties process. This will enable U.S. law enforcement to better assist allies and partners to prosecute cybercriminals. Additionally, the Commission recommends Congress create and fund 12 additional Federal Bureau of Investigation Cyber Assistant Legal Attachés to facilitate intelligence-sharing and help coordinate joint law enforcement actions. Investing in these types of international law enforcement activities improves the credibility of enforcement and signals America's commitment to bring malicious actors to justice.

DETERRENCE BY COST IMPOSITION (PILLAR 6)

A key element of the Commission's strategy entails imposing costs to deter malicious adversary behavior and reduce ongoing adversary activities short of armed conflict. As part of this effort, the Commission puts forth two key recommendations: to conduct a force structure assessment of the Cyber Mission Force; and to conduct a cybersecurity and vulnerability assessments of conventional weapons systems and of the nuclear command, control, and communications enterprise.

Today, the United States has not created credible and sufficient costs against malicious adversary behavior below the level of armed attack—even as the United States has prevented cyberattacks of significant consequences. Our nation must shift from *responding* to malicious behavior after it has already occurred to *proactively* observing, pursuing, and countering adversary operations. This should include imposing costs to change adversary behavior using all instruments of national power, including the military instrument, in accordance with international law.

To achieve these ends, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives in and through cyberspace. The CMF is currently considered at full operational capability (FOC) with 133 teams comprising a total of approximately 6,200 individuals. However, these requirements were defined in 2013, well before our nation experienced or observed some of the key events that have shaped our government's understanding of the cyber threat. The FOC determination for the CMF was also well before the development of the Department of Defense's (DoD) defend forward strategy. Therefore, the

Commission recommends Congress direct the DoD to conduct a force structure assessment of the CMF to ensure the United States has the appropriate force structure and capabilities in light of growing mission requirements. This should include an assessment of the resource implications for intelligence agencies in their combat support agency roles.

If deterrence fails, the United States must also be confident that its military capabilities will work as intended. However, deterrence across all of the domains of warfare is undermined, and the ability of the U.S. to prevail in crisis and conflict is threatened, if adversaries can hold key military systems and functions, including nuclear systems, at risk through cyber means. Therefore, the Commission recommends Congress direct the DoD to conduct a cybersecurity vulnerability assessment of all segments of nuclear command, control, and communications systems and continually assess weapon systems' cyber vulnerabilities.

Our hope is that, by implementing these recommendations, we can ensure our nation is willing and able to counter and reduce malicious adversary behavior below the level of armed conflict, impose costs to deter significant cyberattacks, and, if necessary, fight and win in crisis and conflict.

CONCLUSION

The recommendations put forward by the Commission represent important first steps toward reducing adversaries' ability and willingness to exploit cyberspace to undermine American interests and values. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. Cyber operations have become a weapon of choice for adversaries seeking to hold the U.S. economy and national security at risk. Near-peer adversaries such as China and Russia are attempting to reassert their influence regionally and globally, using cyber and information operations to undermine American security interests. The concept of deterrence must evolve to address this new strategic landscape. Reducing the scope and severity of these adversary cyber operations and campaigns requires adopting the Commission's strategy of layered cyber deterrence.