UNITED STATES OF AMERICA

CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

MARCH 2020

EXECUTIVE SUMMARY

CHAIRMEN'S LETTER

Our country is at risk, not only from a catastrophic cyberattack but from millions of daily intrusions disrupting everything from financial transactions to the inner workings of our electoral system. Capturing the complexity of this challenge is hard. Even the man credited with inventing the term "cyberspace," the science fiction author William Gibson, would later criticize it as an "evocative and essentially meaningless" buzzword.[1]

In studying this issue, it is easy to descend into a morass of classification, acronyms, jargon, and obscure government organization charts. To avoid that, we tried something different: an unclassified report that we hope will be found readable by the very people who are affected by cyber insecurity—*everyone*. This report is also aimed squarely at **action**; it has numerous recommendations addressing organizational, policy, and technical issues, and we included an appendix with draft bills that Congress can rapidly act upon to put these ideas into practice and make America more secure.

The reality is that we are dangerously insecure in cyber. Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process, and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state-sponsored intellectual property theft using cyber espionage. A major cyberattack on the nation's critical infrastructure and economic system would create chaos and lasting damage exceeding that wreaked by fires in California, floods in the Midwest, and hurricanes in the Southeast.

To prevent this from happening, our report outlines a new cyber strategy and provides more than 75 recommendations for action across the public and private sectors. Here are some big ideas to get the conversation started.

First, **deterrence is possible in cyberspace**. Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure. In other words, through our inability or unwillingness to identify and punish our cyber adversaries, we are signaling that interfering in American elections or stealing billions in U.S. intellectual property is acceptable. The federal government and the private sector must defend themselves and strike back with **speed and agility**. This is difficult because the government is not optimized to be quick or agile, but we simply must be faster than our adversaries in order to prevent them from destroying our networks and, by extension, our way of life. Our strategy of *layered cyber deterrence* is designed with this goal in mind. It combines enhanced resilience with enhanced attribution capabilities and a clearer signaling strategy with collective action by our partners and allies. It is a simple framework laying out how we evolve into a hard target, a good ally, and a bad enemy.

Second, **deterrence relies on a resilient economy**. During the Cold War, our best minds were tasked with developing Continuity of Government plans to ensure that the government could survive and the nation recover after a nuclear strike. We need similar planning today to ensure that we can reconstitute in the aftermath of a national-level cyberattack. We also need to ensure that our economy continues to run. We recommend that the government institute a Continuity of the Economy plan to ensure that we can rapidly restore critical functions across corporations and industry sectors, and get the economy back up and running after a catastrophic cyberattack. Such a plan is a fundamental pillar of deterrence—a way to tell our adversaries that we, as a society, will survive to defeat them with **speed and agility** if they launch a major cyberattack against us.

Third, **deterrence requires government reform.** We need to elevate and empower existing cyber agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA), and create new focal points for coordinating cybersecurity in the executive branch and Congress. To that end, we recommend the creation of a National Cyber Director with oversight from new congressional Cybersecurity Committees, but our goal is not to create more bureaucracy with new and duplicative roles and organizations. Rather, we propose giving existing organizations the tools they need to act with **speed and agility** to defend our networks and impose costs on our adversaries. The key is CISA, which we have tried to empower as the lead agency for federal cybersecurity and the private sector's preferred partner. We want working at CISA to become so appealing to young professionals interested in national service that it competes with the NSA, the FBI, Google, and Facebook for top-level talent (and wins).

Fourth, **deterrence will require private-sector entities to step up and strengthen their security posture**. Most of our critical infrastructure is owned by the private sector. That is why we make certain recommendations, such as establishing a cloud security certification or modernizing corporate accountability reporting requirements. We do not want to saddle the private sector with onerous and counterproductive regulations, nor do we want to force companies to hand over their data to the federal government. We are not the Chinese Communist Party, and indeed our best path to beating our adversaries is to stay free and innovative. But we need C-suite executives to take cyber seriously since they are on the front lines. With support from the federal government, private-sector entities must be able to act with **speed and agility** to stop cyberattackers from breaking out in their networks and the larger array of networks on which the nation relies.

Fifth, **election security must become a priority**. The American people still do not have the assurance that our election systems are secure from foreign manipulation. If we don't get election security right, deterrence will fail and future generations will look back with longing and regret on the once powerful American Republic and wonder how we screwed the whole thing up. We believe we need to continue appropriations to fund election infrastructure modernization at the state and local levels. At the same time, states and localities need to pay their fair share to secure elections, and they can draw on useful resources—such as nonprofits that can act with greater **speed and agility** across all 50 states—to secure elections from the bottom up rather than waiting for top-down direction and funding. We also need to ensure that regardless of the

method of casting a vote, paper or electronic, a paper audit trail exists (and yes, we recognize the irony of a cyber commission recommending a paper trail).

We didn't solve everything in this report. We didn't even agree on everything. There are areas, such as balancing maximum encryption versus mandatory lawful access to devices, where the best we could do was provide a common statement of principles. Yet every single Commissioner was willing to make compromises in the course of our work because we were all united by the recognition that the status quo is not getting the job done. The status quo is inviting attacks on America every second of every day. The status quo is a slow surrender of American power and responsibility. We all want that to stop. So please do us, and your fellow Americans, a favor. Read this report and then demand that your government and private sector leadership act with **speed and agility** to secure our cyber future.

Senator Angus King (I-Maine)
Co-Chairman
Cyberspace Solarium Commission

Representative Mike Gallagher (R-Wisconsin)
Co-Chairman
Cyberspace Solarium Commission

EXECUTIVE SUMMARY

AN URGENT CALL TO ACTION

For over 20 years, nation-states and non-state actors have used cyberspace to subvert American power, American security, and the American way of life. Despite numerous criminal indictments, economic sanctions, and the development of robust cyber and non-cyber military capabilities, the attacks against the United States have continued. The perpetrators saw that their onslaught damaged the United States without triggering a significant retaliation. Chinese cyber operators stole hundreds of billions of dollars in intellectual property to accelerate China's military and economic rise and undermine U.S. military dominance.[2] Russian operators and their proxies damaged public trust in the integrity of American elections and democratic institutions.[3] China, Russia, Iran, and North Korea all probed U.S. critical infrastructure with impunity. Criminals leveraged globally connected networks to steal assets from individuals, companies, and governments. Extremist groups used these networks to raise funds and recruit followers, increasing transnational threats and insecurity. American restraint was met with unchecked predation.[4]

The digital connectivity that has brought economic growth, technological dominance, and an improved quality of life to nearly every American has also created a strategic dilemma. The more digital connections people make and data they exchange, the more opportunities adversaries have to destroy private lives, disrupt critical infrastructure, and damage our economic and democratic institutions. The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide. Moreover, shortfalls in agility, technical expertise, and unity of effort, both within the U.S. government and between the public and private sectors, are growing.

The 2019 National Defense Authorization Act chartered the U.S. Cyberspace Solarium Commission to address this challenge. The President and Congress tasked the Commission to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy?

THE STRATEGY

After conducting an extensive study including over 300 interviews, a competitive strategy event modeled after the original Project Solarium in the Eisenhower administration, and stress tests by external red teams, the Commission advocates a new strategic approach to cybersecurity: **layered cyber deterrence**. The desired end state of layered cyber deterrence is a reduced probability and impact of cyberattacks of significant consequence. The strategy outlines three ways to achieve this end state:

1. *Shape behavior.* The United States must work with allies and partners to promote responsible behavior in cyberspace.
2. *Deny benefits.* The United States must deny benefits to adversaries who have long exploited cyberspace to their advantage, to American disadvantage, and at little cost to themselves. This new approach requires securing critical networks in collaboration with the private sector to promote national resilience and increase the security of the cyber ecosystem.
3. *Impose costs.* The United States must maintain the capability, capacity, and credibility needed to retaliate against actors who target America in and through cyberspace.

Each of the three ways described above involves a deterrent layer that increases American public- and private-sector security by altering how adversaries perceive the costs and benefits of using cyberspace to attack American interests. These three deterrent layers are supported by six policy pillars that organize more than 75 recommendations. These pillars represent the means to implement layered cyber deterrence.

While deterrence is an enduring American strategy, there are two factors that make layered cyber deterrence bold and distinct. First, the approach prioritizes deterrence by denial, specifically by increasing the defense and security of cyberspace through resilience and public- and private-sector collaboration. Reducing the vulnerabilities adversaries can target denies them opportunities to attack American interests through cyberspace. Second, the strategy incorporates the concept of "defend forward" to reduce the frequency and severity of attacks in cyberspace that do not rise to a level that would warrant the full spectrum of retaliatory responses, including military responses. Though the concept originated in the Department of Defense, the Commission integrates defend forward into a national strategy for securing cyberspace using all the instruments of power. Defend forward posits that to disrupt and defeat ongoing adversary campaigns, the United States must proactively observe, pursue, and counter adversaries' operations and impose costs short of armed conflict. This posture signals to adversaries that the U.S. government will respond to cyberattacks, even those below the level of armed conflict that do not cause physical destruction or death, with all the tools at its disposal and consistent with international law.

THE IMPLEMENTATION

Foundation: Government Reform

The three layers of cyber deterrence rest on a common foundation: the need to reform how the U.S. government is organized to secure cyberspace and respond to attacks. The U.S. government is currently not designed to act with the speed and agility necessary to defend the country in cyberspace. We must get faster and smarter, improving the government's ability to organize concurrent, continuous, and collaborative efforts to build resilience, respond to cyber threats, and preserve military options that signal a capability and willingness to impose costs on adversaries. Reformed government oversight and organization that is properly resourced and staffed,

in alignment with a strategy of layered cyber deterrence, will enable the United States to reduce the probability, magnitude, and effects of significant attacks on its networks.

Pillar: *Reform the U.S. Government's Structure and Organization for Cyberspace.* While cyberspace has transformed the American economy and society, the government has not kept up. Existing government structures and jurisdictional boundaries fracture cyber policymaking processes, limit opportunities for government action, and impede cyber operations. Rapid, comprehensive improvements at all levels of government are necessary to change these dynamics and ensure that the U.S. government can protect the American people, their way of life, and America's status as a global leader. Major recommendations in this pillar are:

- The executive branch should **issue an updated National Cyber Strategy (1.1)** that reflects the strategic approach of layered cyber deterrence and emphasizes resilience, public-private collaboration, and defend forward as key elements.

- Congress should **establish House Permanent Select and Senate Select Committees on Cybersecurity (1.2)** to provide integrated oversight of the cybersecurity efforts dispersed across the federal government.

- Congress should **establish a Senate-confirmed National Cyber Director (NCD) (1.3)**, supported by an Office of the NCD, within the Executive Office of the President. The NCD will be the President's principal advisor for cybersecurity-related issues, as well as lead national-level coordination of cybersecurity strategy and policy, both within government and with the private sector.

- Congress should **strengthen the Cybersecurity and Infrastructure Security Agency (CISA) (1.4)** in its mission to ensure the national resilience of critical infrastructure, promote a more secure cyber ecosystem, and serve as the central coordinating element to support and integrate federal, state and local, and private-sector cybersecurity efforts. Congress must invest significant resources in CISA and provide it with clear authorities to realize its full potential.

- Congress and the executive branch should pass legislation and **implement policies designed to better recruit, develop, and retain cyber talent (1.5)** while acting to deepen the pool of candidates for cyber work in the federal government.

Layer 1: Shape Behavior

In the first layer, the strategy calls for shaping responsible behavior and encouraging restraint in cyberspace by strengthening norms and non-military instruments. Effective norms will not emerge without American leadership. For this reason, the United States needs to build a coalition of partners and allies to secure its shared interests and values in cyberspace.

Pillar: *Strengthen Norms and Non-military Tools.* A system of norms, built through international engagement and cooperation, promotes responsible behavior and, over time, dissuades adversaries from using cyber operations to undermine any nation's interests. The United States and others have agreed to norms of responsible behavior for cyberspace, but they go largely unenforced today. The United States can strengthen the current system of cyber norms by using non-military tools, including law enforcement actions, sanctions, diplomacy, and information sharing, to more effectively persuade states to conform to these norms and punish those who violate them. Such punishment requires developing the ability to quickly and accurately attribute cyberattacks. Building a coalition of like-minded allies and partners willing to collectively use these instruments to support a rules-based international order in cyberspace will better hold malign actors accountable. The major recommendations in this pillar are:

- Congress should **create an Assistant Secretary of State (2.1)** in the Department of State, with a new Bureau of Cyberspace Security and Emerging Technologies, who will lead the U.S. government effort to develop and reinforce international norms in cyberspace. This will help promote international norms that support and reflect U.S. interests and values while creating benefits for responsible state behavior through engagement with allies and partners.

- The executive branch should **engage actively and effectively in forums setting international information and communications technology standards (2.1.2).** Specifically, the National Institute of Standards and Technology should facilitate robust and integrated participation by the federal government, academia, professional societies, and industry.

- Congress should take steps to **improve international tools for law enforcement activities in cyberspace (2.1.4),** including streamlining the Mutual Legal Assistance Treaty and Mutual Legal Assistance Agreement process and increasing the number of FBI Cyber Assistant Legal Attachés.

Layer 2: Deny Benefits

In the second layer, the strategy calls for denying benefits to adversaries by promoting national resilience, reshaping the cyber ecosystem, and advancing the government's relationship with the private sector to establish an enhanced level of common situational awareness and joint collaboration. The United States needs a whole-of-nation approach to secure its interests and institutions in cyberspace.

Pillar: *Promote National Resilience.* Resilience—the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior—is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends. National resilience efforts rely on the ability of the United States, in both the public and private sectors, to accurately identify, assess, and mitigate risk across all elements of critical infrastructure. The nation must be sufficiently prepared to respond to and recover from an attack, sustain critical functions even under degraded

conditions, and, in some cases, restart critical functionality after disruption. Major recommendations in this pillar are:

- Congress should **codify responsibilities and ensure sufficient resources (3.1)** for the Cybersecurity and Infrastructure Security Agency and sector-specific agencies **in the identification, assessment, and management of national and sector-specific risk**.

- Congress should direct the U.S. government to **develop and maintain Continuity of the Economy planning (3.2)** in consultation with the private sector to ensure continuous operation of critical functions of the economy in the event of a significant cyber disruption.

- Congress should **codify a Cyber State of Distress** tied to a **Cyber Response and Recovery Fund (3.3)** to ensure sufficient resources and capacity to respond rapidly to significant cyber incidents.

- Congress should **improve the structure and sustain the funding of the Election Assistance Commission (3.4)**, enabling it to increase its operational capacity to support states and localities in defense of the digital election infrastructure that underpins federal elections and to ensure the widest use of voter-verifiable, auditable, and paper-based voting systems.

- The U.S. government should **promote digital literacy, civics education, and public awareness (3.5)** to build societal resilience to foreign, malign cyber-enabled information operations.

Pillar: *Reshape the Cyber Ecosystem toward Greater Security.* Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities. Over time, this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes. In some cases, that requires aligning market forces. In other cases, where those forces either are not present or do not adequately address risk, the U.S. government must explore legislation, regulation, executive action, and public- as well as private-sector investments. Major recommendations in this pillar are:

- Congress should **establish and fund a National Cybersecurity Certification and Labeling Authority (4.1)** empowered to **establish and manage a program on security certifications and labeling** of information and communications technology products.

- Congress should **pass a law establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities (4.2)** for as long as they support a product or service.

- Congress should **establish a Bureau of Cyber Statistics (4.3)** charged with **collecting and providing statistical data on cybersecurity** and the cyber ecosystem to inform policymaking and government programs.

- Congress should resource and direct the Department of Homeland Security to **fund a federally funded research and development center (4.4)** to work with state-level regulators to **develop certifications for cybersecurity insurance products**.

- The National Cybersecurity Certification and Labeling Authority should **develop a cloud security certification (4.5)**, in consultation with the National Institute of Standards and Technology, the Office of Management and Budget, and the Department of Homeland Security.

- Congress should direct the U.S. government to **develop and implement an industrial base strategy for information and communications technology to ensure trusted supply chains (4.6)** and the availability of critical information and communications technologies.

- Congress should **pass a national data security and privacy protection law (4.7)** establishing and standardizing requirements for the collection, retention, and sharing of user data.

Pillar: *Operationalize Cybersecurity Collaboration with the Private Sector.* Unlike in other physical domains, in cyberspace the government is often not the primary actor. Instead, it must support and enable the private sector. The government must build and communicate a better understanding of threats, with the specific aim of informing private-sector security operations, directing government operational efforts to counter malicious cyber activities, and ensuring better common situational awareness for collaborative action with the private sector. Further, while recognizing that private-sector entities have primary responsibility for the defense and security of their networks, the U.S. government must bring to bear its unique authorities, resources, and intelligence capabilities to support these actors in their defensive efforts. Major recommendations in this pillar are:

- Congress should **codify the concept of "systemically important critical infrastructure" (5.1)**, whereby entities responsible for systems and assets that underpin national critical functions are ensured the full support of the U.S. government and shoulder additional security requirements befitting their unique status and importance.

- Congress should **establish and fund a Joint Collaborative Environment (5.2)**, a common and interoperable environment for **sharing and fusing threat information, insights, and other relevant data** across the federal government and between the public and private sectors.

- Congress should direct the executive branch to **strengthen a public-private, integrated cyber center in CISA (5.3)** to support its critical infrastructure security and resilience mission and to **conduct a one-year, comprehensive systems analysis review of federal cyber and cybersecurity centers**.

- The executive branch should establish a **Joint Cyber Planning Cell (5.4)** under CISA to coordinate cybersecurity planning and readiness across the federal government and between the public and private sectors.

Layer 3: Impose Costs

In the final layer, the strategy outlines how to impose costs to deter future malicious behavior and reduce ongoing adversary activities short of armed conflict through the employment of all instruments of power in the defense of cyberspace, including systemically important critical infrastructure. A key, but not the only, element of cost imposition is the military instrument of power. Therefore, the United States must maintain the capacity, resilience, and readiness to employ cyber and non-cyber capabilities across the spectrum of engagement from competition to crisis and conflict. The United States needs ready and resilient capabilities to thwart and respond to adversary action.

Pillar: *Preserve and Employ the Military Instrument of Power—and All Other Options to Deter Cyberattacks at Any Level.* Cyberspace is already an arena of strategic competition, where states project power, protect their interests, and punish their adversaries. Future contingencies and conflicts will almost certainly contain a cyber component. In this environment, the United States must defend forward to limit malicious adversary behavior below the level of armed attack, deter conflict, and, if necessary, prevail by employing the full spectrum of its capabilities, using all the instruments of national power. Examples of adversary actions below armed attack include cyber-enabled attacks on the U.S. election systems or cyber-enabled intellectual property theft. To achieve these ends, the U.S. government 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 the United States in cyberspace. Furthermore, conventional weapons and nuclear capabilities require cybersecurity and resilience to ensure that the United States preserves credible deterrence and the full range of military response options. The United States must be confident that its military capabilities will work as intended. Finally, across the spectrum of engagement from competition to crisis and conflict, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives in and through cyberspace. This demands sufficient capacity, capabilities, and streamlined decision-making processes to enable rapid and effective cyber response options to impose costs against adversaries. Major recommendations in this pillar include:

- Congress should direct the Department of Defense to **conduct a force structure assessment of the Cyber Mission Force (6.1)** to ensure that the United States has the appropriate force structure and capabilities in light of growing mission requirements and increasing expectations, in both scope and scale. This should include an assessment of the resource implications for the National Security Agency in its combat support agency role.

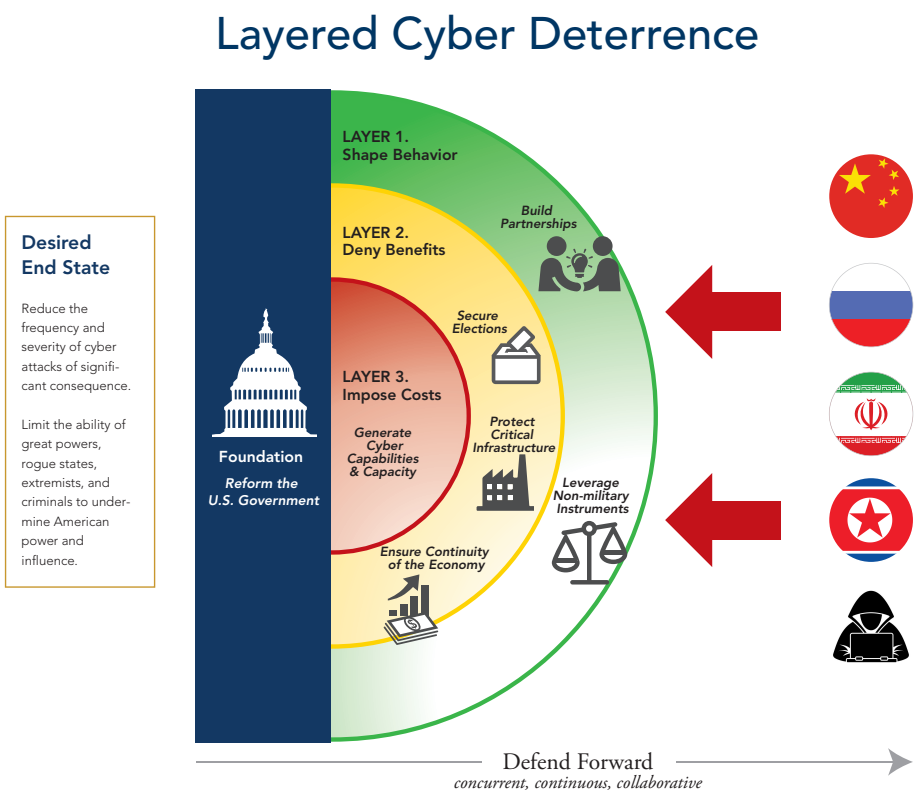
- Congress should direct the Department of Defense to **conduct a cybersecurity vulnerability assessment of all segments of the nuclear control systems and continually assess weapon systems' cyber vulnerabilities (6.2)**.

- Congress should require **Defense Industrial Base (DIB) participation in threat intelligence sharing programs (6.2.1) and threat hunting on DIB networks (6.2.2)**.

THE WAY FORWARD

The status quo in cyberspace is unacceptable. The current state of affairs invites aggression and establishes a dangerous pattern of actors attacking the United States without fear of reprisal. Adversaries are increasing their cyber capabilities while U.S. vulnerabilities continue to grow. There is much that the U.S. government can do to improve its defenses and reduce the risk of a significant attack, but it is clear that government action alone is not enough. Most of the critical infrastructure that drives the American economy, spurs technological innovation, and supports the U.S. military resides in the private sector. If the U.S. government cannot find a way to seamlessly collaborate with the private sector to build a resilient cyber ecosystem, the nation will never be secure. And, eventually, a massive cyberattack could lead to large-scale physical destruction, sparking a response of haphazard government overreach that stifles innovation in the digital economy and further erodes American strength.

To avoid these outcomes, the U.S. government must move to adopt the new strategy detailed in this report—layered cyber deterrence—and the more than 75 recommendations designed to make this approach a reality. The executive branch and Congress should give these recommendations and the associated legislative proposals close consideration. Congress should also consider ways to monitor, assess, and report on the implementation of this report's recommendations over the next two years.



ROLL-UP OF RECOMMENDATIONS

PILLAR 1: REFORM THE U.S. GOVERNMENT'S STRUCTURE AND ORGANIZATION FOR CYBERSPACE

Key Recommendation 1.1: Issue an Updated National Cyber Strategy

- Enabling Recommendation 1.1.1: Develop a Multitiered Signaling Strategy
- Enabling Recommendation 1.1.2: Promulgate a New Declaratory Policy

Key Recommendation 1.2: Create House Permanent Select and Senate Select Committees on Cybersecurity

- Enabling Recommendation 1.2.1: Reestablish the Office of Technology Assessment

Key Recommendation 1.3: Establish a National Cyber Director

Key Recommendation 1.4: Strengthen the Cybersecurity and Infrastructure Security Agency

- Enabling Recommendation 1.4.1: Codify and Strengthen the Cyber Threat Intelligence Integration Center
- Enabling Recommendation 1.4.2: Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force

Key Recommendation 1.5: Diversify and Strengthen the Federal Cyberspace Workforce

- Enabling Recommendation 1.5.1: Improve Cyber-Oriented Education

PILLAR 2: STRENGTHEN NORMS AND NON-MILITARY TOOLS

Key Recommendation 2.1: Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State

- Enabling Recommendation 2.1.1: Strengthen Norms of Responsible State Behavior in Cyberspace
- Enabling Recommendation 2.1.2: Engage Actively and Effectively in Forums Setting International Information and Communications Technology Standards
- Enabling Recommendation 2.1.3: Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance
- Enabling Recommendation 2.1.4: Improve International Tools for Law Enforcement Activities in Cyberspace
- Enabling Recommendation 2.1.5: Leverage Sanctions and Trade Enforcement Actions

Enabling Recommendation 2.1.6: Improve Attribution Analysis and the Attribution-Decision Rubric

Enabling Recommendation 2.1.7: Reinvigorate Efforts to Develop Cyber Confidence-Building Measures

PILLAR 3: PROMOTE NATIONAL RESILIENCE

Key Recommendation 3.1: Codify Sector-specific Agencies into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk

Enabling Recommendation 3.1.1: Establish a Five-Year National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy

Enabling Recommendation 3.1.2: Establish a National Cybersecurity Assistance Fund to Ensure Consistent and Timely Funding for Initiatives That Underpin National Resilience

Key Recommendation 3.2: Develop and Maintain Continuity of the Economy Planning

Key Recommendation 3.3: Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"

Enabling Recommendation 3.3.1: Designate Responsibilities for Cybersecurity Services under the Defense Production Act

Enabling Recommendation 3.3.2: Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts

Enabling Recommendation 3.3.3: Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts

Enabling Recommendation 3.3.4: Expand Coordinated Cyber Exercises, Gaming, and Simulation

Enabling Recommendation 3.3.5: Establish a Biennial National Cyber Tabletop Exercise

Enabling Recommendation 3.3.6: Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard

Key Recommendation 3.4: Improve the Structure and Enhance Funding of the Election Assistance Commission

Enabling Recommendation 3.4.1: Modernize Campaign Regulations to Promote Cybersecurity

Key Recommendation 3.5: Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations

Enabling Recommendation 3.5.1: Reform Online Political Advertising to Defend against Foreign Influence in Elections

PILLAR 4: RESHAPE THE CYBER ECOSYSTEM TOWARD GREATER SECURITY

Key Recommendation 4.1: Establish and Fund a National Cybersecurity Certification and Labeling Authority

- Enabling Recommendation 4.1.1: Create or Designate Critical Technology Security Centers
- Enabling Recommendation 4.1.2: Expand and Support the National Institute of Standards and Technology Security Work

Key Recommendation 4.2: Establish Liability for Final Goods Assemblers

- Enabling Recommendation 4.2.1: Incentivize Timely Patch Implementation

Key Recommendation 4.3: Establish a Bureau of Cyber Statistics

Key Recommendation 4.4: Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications

- Enabling Recommendation 4.4.1: Establish a Public-Private Partnership on Modeling Cyber Risk
- Enabling Recommendation 4.4.2: Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events
- Enabling Recommendation 4.4.3: Incentivize Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities
- Enabling Recommendation 4.4.4: Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements

Key Recommendation 4.5: Develop a Cloud Security Certification

- Enabling Recommendation 4.5.1: Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments
- Enabling Recommendation 4.5.2: Develop a Strategy to Secure Foundational Internet Protocols and Email
- Enabling Recommendation 4.5.3: Strengthen the U.S. Government's Ability to Take Down Botnets

Key Recommendation 4.6: Develop and Implement an Information and Communications Technology Industrial Base Strategy

- Enabling Recommendation 4.6.1: Increase Support to Supply Chain Risk Management Efforts
- Enabling Recommendation 4.6.2: Commit Significant and Consistent Funding toward Research and Development in Emerging Technologies
- Enabling Recommendation 4.6.3: Strengthen the Capacity of the Committee on Foreign Investment in the United States
- Enabling Recommendation 4.6.4: Invest in the National Cyber Moonshot Initiative

Key Recommendation 4.7: Pass a National Data Security and Privacy Protection Law

Enabling Recommendation 4.7.1: Pass a National Breach Notification Law

PILLAR 5: OPERATIONALIZE CYBERSECURITY COLLABORATION WITH THE PRIVATE SECTOR

Key Recommendation 5.1: Codify the Concept of "Systemically Important Critical Infrastructure"

Enabling Recommendation 5.1.1: Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector

Enabling Recommendation 5.1.2: Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities

Enabling Recommendation 5.1.3: Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities

Key Recommendation 5.2: Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information

Enabling Recommendation 5.2.1: Expand and Standardize Voluntary Threat Detection Programs

Enabling Recommendation 5.2.2: Pass a National Cyber Incident Reporting Law

Enabling Recommendation 5.2.3: Amend the Pen Register Trap and Trace Statute to Enable Better Identification of Malicious Actors

Key Recommendation 5.3: Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers

Key Recommendation 5.4: Establish a Joint Cyber Planning Cell under the Cybersecurity and Infrastructure Security Agency

Enabling Recommendation 5.4.1: Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives

Enabling Recommendation 5.4.2: Expand Cyber Defense Collaboration with Information and Communications Technology Enablers

PILLAR 6: PRESERVE AND EMPLOY THE MILITARY INSTRUMENT OF POWER

Key Recommendation 6.1: Direct the Department of Defense to Conduct a Force Structure Assessment of the Cyber Mission Force

- Enabling Recommendation 6.1.1: Direct the Department of Defense to Create a Major Force Program Funding Category for U.S. Cyber Command
- Enabling Recommendation 6.1.2: Expand Current Malware Inoculation Initiatives
- Enabling Recommendation 6.1.3: Review the Delegation of Authorities for Cyber Operations
- Enabling Recommendation 6.1.4: Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces
- Enabling Recommendation 6.1.5: Cooperate with Allies and Partners to Defend Forward
- Enabling Recommendation 6.1.6: Require the Department of Defense to Define Reporting Metrics
- Enabling Recommendation 6.1.7: Assess the Establishment of a Military Cyber Reserve
- Enabling Recommendation 6.1.8: Establish Title 10 Professors in Cyber Security and Information Operations

Key Recommendation 6.2: Conduct a Cybersecurity Vulnerability Assessment of All Segments of the NC3 and NLCC Systems and Continually Assess Weapon Systems' Cyber Vulnerabilities

- Enabling Recommendation 6.2.1: Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program
- Enabling Recommendation 6.2.2: Require Threat Hunting on Defense Industrial Base Networks
- Enabling Recommendation 6.2.3: Designate a Threat-Hunting Capability across the Department of Defense Information Network
- Enabling Recommendation 6.2.4: Assess and Address the Risk to National Security Systems Posed by Quantum Computing

NOTES

EXECUTIVE SUMMARY

1 See the documentary *No Maps for These Territories*, directed by Mark Neale (Vancouver, CA: Docurama, 2000).

2 The White House, "National Cyber Strategy of the United States of America" (September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

3 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," Journal of Strategic Studies, no. 42 (2019): 212–34.

4 David Alexander, "Hagel, Ahead of China Trip, Urges Military Restraint in Cyberspace," *Reuters,* March 28, 2014, https://www.reuters.com/article/us-usa-defense-cybersecurity/hagel-ahead-of-china-trip-urges-military-restraint-in-cyberspace-idUSBREA2R1ZH20140328.

COMMISSIONERS

CO-CHAIRMEN

Angus S. King Jr.	U.S. Senator for Maine
Michael "Mike" J. Gallagher	U.S. Representative for Wisconsin's 8th District

COMMISSIONERS

Frank J. Cilluffo	Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security
Thomas A. "Tom" Fanning	Chairman, President, and Chief Executive Officer of Southern Company
Andrew Hallman	Principal Executive of the Office of the Director of National Intelligence performing the duties of the Principal Deputy Director of National Intelligence
John C. "Chris" Inglis	U.S. Naval Academy Looker Professor for Cyber Security Studies and Former Deputy Director of the National Security Agency
James R. "Jim" Langevin	U.S. Representative for Rhode Island's 2nd District
Patrick J. Murphy	Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District
David L. Norquist	Deputy Secretary of Defense
David Pekoske	Administrator of the Transportation Security Administration & Senior Official Performing the Duties of the Deputy Secretary of Homeland Security
Samantha F. Ravich	Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies
Benjamin E. "Ben" Sasse	U.S. Senator for Nebraska
Suzanne E. Spaulding	Senior Adviser for Homeland Security at the Center for Strategic and International Studies and former Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security
Christopher Wray	Director of the Federal Bureau of Investigation

The executive branch Commissioners contributed superb assessments, insights, and recommendations to the report and actively participated in the Commission's deliberations, but, in accordance with executive branch legal guidance, abstained from its final approval.

STAFF

SENIOR STAFF

Mark Montgomery	Executive Director
Deborah Grays	Chief of Staff
Erica Borghard	Senior Director and Task Force One Lead
John Costello	Senior Director and Task Force Two Lead
Val Cofield	Senior Director and Task Force Three Lead
Cory Simpson	Senior Director and Directorate Four Lead
Benjamin Jensen	Senior Research Director and Lead Writer

FULL TIME STAFF

Laura Bate, Director for Cyber Engagement

Phoebe Benich, Cyber Strategy and Policy Analyst

Tatyana Bolton, Policy Director

Gregory Buck, Deputy Chief of Staff

Madison Creery, Cyber Strategy and Policy Analyst

Matthew Ferren, Cyber Strategy and Policy Analyst

Chris Forshey, Facility Security Officer

Michael Garcia, Director of External Engagement and Outreach

Charles Garzoni, Director for Defensive Strategy

Karrie Jefferson, Director for Cyber Engagement

Ainsley Katz, Cyber Strategy and Policy Analyst

Alison King, Strategic Communications and Congressional Advisor

Timothy Kocher, Cyber Strategist

Noah Komnick, Cyber Strategist

Harry Krejsa, Director and Deputy Team Lead

Sang Lee, Director for Cyber Engagement

Robert Morgus, Director for Research and Analysis

Diane Pinto, Cyber Strategy and Policy Analyst

Matthew Smith, Cyber Strategist

Brandon Valeriano, Senior Advisor

Dave Zikusoka, Policy Director

LEGAL ADVISORS

Stefan Wolfe, General Counsel

Corey Bradley, Deputy General Counsel

Cody Cheek, Legal Advisor

David Simon, Chief Counsel for Cybersecurity and National Security

Veronica Glick, Deputy Chief Counsel for Cybersecurity and National Security

Joshua Silverstein, Deputy Chief Counsel for Cybersecurity and National Security

PRODUCTION SUPPORT

Alice Falk, Editor

Laurel Prucha Moran, Graphic Designer


U.S. CYBERSPACE SOLARIUM COMMISSION