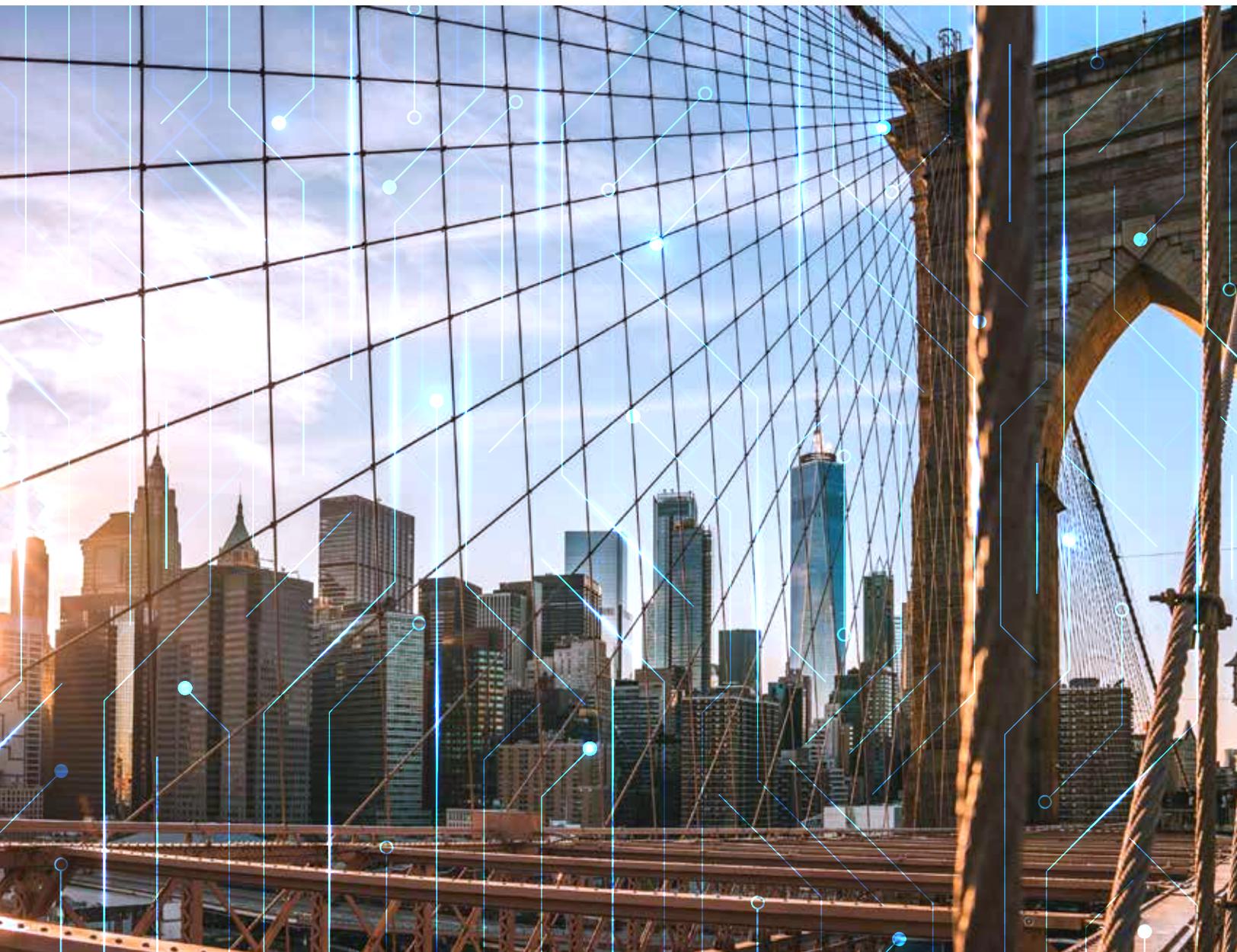


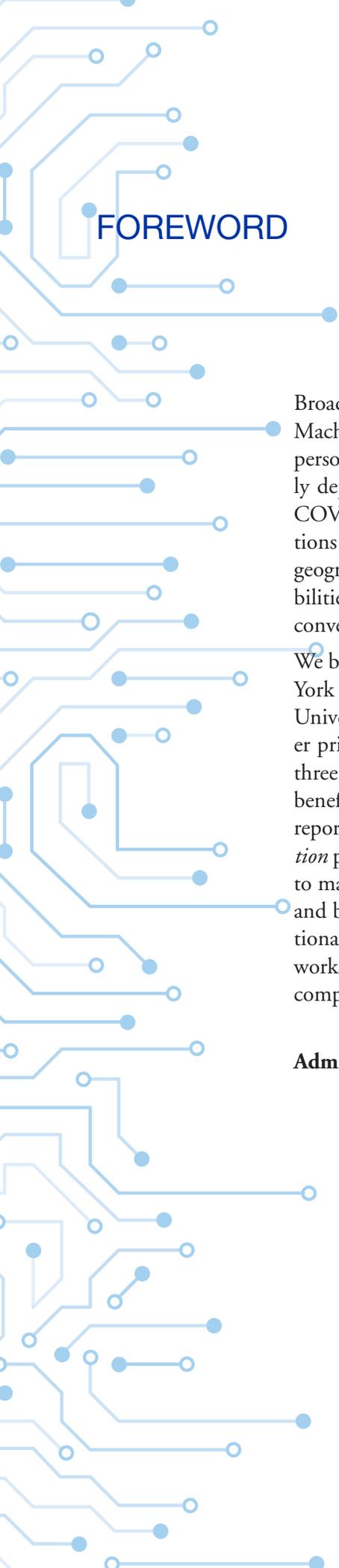
Enhancing Readiness for National Cyber Defense through Operational Collaboration

NEW YORK CYBER TASK FORCE



CONTENTS

Foreword	3	Appendixes	30
Members of the New York Cyber Task Force	4	Appendix 1: Establishing a National Cyber Crisis Contingency Identification Program	31
Executive Summary	5	Appendix 2: Map of Drivers to Scenarios	33
Introduction	6	Appendix 3: Scenarios	47
NYCTF Analytical Approach and Activities	8	Appendix 4: Workshop Findings	49
Recommendations to Enhance National Cyber Response Readiness	11	Appendix 5: Solarium Commission and NDAA Observations	60
Recommendation 1: Identify National Cyber Crisis Contingencies	12	Notes	61
Recommendation 2: Establish a National Cyber Response Network	14		
Recommendation 3: Operation of the NCRN	16		
Recommendation 4: Assess National Cyber Response Capabilities to Ensure Readiness	17		
Recommendation 5: Ensure National Cyber Readiness through Training and Exercises	19		
Enabling Operational Readiness	20		
Enabling Recommendation 1: Establish Integrated Cyber Crisis Information Networks	20		
Enabling Recommendation 2: Address Technology Evolution to Ensure Readiness	21		
Enabling Recommendation 3: Remove Legal and Procedural Barriers to Enhance Response	23		
Enabling Recommendation 4: Build Trust and Confidence for Cyber Crisis Response	25		
Enabling Recommendation 5: Close Resource Gaps to Ensure Readiness	27		
Conclusion	29		



FOREWORD

Broadband from space, 5G, the Internet of Things, artificial intelligence, and Machine Learning—the information revolution is gaining speed and effect. Our personal lives, businesses, governments, and safety are all becoming increasingly dependent on Internet-based connections. Digital growth is only accelerating as COVID-19 increases reliance on the cyber ecosystem. Impressive as these applications are, the cyber threat is proceeding at an even faster pace that does not recognize geographic boundaries, and every beneficial new development brings greater vulnerabilities. To an increasing extent, malignant cyber activity now threatens not only our convenience but also our wealth and safety.

We both were asked to serve as advisers and to participate in the activities of the New York Cyber Task Force on operational collaboration. We commend the Columbia University School of International and Public Affairs for continuing to bring together private, public, and academic leaders to address the difficult issues. These are the three groups that must integrate their knowledge, plans, and actions to preserve the benefits of the information revolution, while dealing with the threats. The NYCTF report *Enhancing Readiness for National Cyber Defense through Operational Collaboration* provides insights into the challenges and thoughtful, practical recommendations to make progress. Our government and private leadership both have responsibilities, and both must act together along the lines presented in this report to establish a national cyber response network that will both increase the security of information networks and respond to successful attacks. Today's fragmented, patchwork defenses are completely inadequate. We must invest now in readiness to secure our digital future.

Admiral Dennis C. Blair

Admiral Michael S. Rogers

MEMBERS OF THE NEW YORK CYBER TASK FORCE

Dmitri Alperovitch – Silverado Policy Accelerator

John Bansemer – Georgetown University

Dennis C. Blair – Former U.S. Director of National Intelligence

Erica Borghard – Atlantic Council

Michael Bradshaw – NBC Universal

Rico Brandenburg – Oliver Wyman

Geoff Brown – City of New York

Chris Button – Analysis and Resilience Center for Systemic Risk

Byron Collie – JP Morgan Chase

John Costello – Cyberspace Solarium Commission

Michael Daniel – Cyber Threat Alliance

Scott DePasquale – Analysis and Resilience Center for Systemic Risk

Daniel Dobrygowski – World Economic Forum

Benjamin Flatgard – JP Morgan Chase

David Forscey – The Aspen Institute

Thomas Fuhrman – VECTORmv

Nathaniel Gleicher – Facebook

Eric Goldstein – Goldman Sachs

Josh Harriman – Rapid 7

Jason Healey – Columbia University

Justin Henck – Facebook

Trey Herr – Atlantic Council

Niloofar Howe – Energy Impact Partners

Merit Janow – Columbia University†

Kristin Judge – Cybercrime Support Network

Elsa Kania – Center for New American Security

Elena Kvochko – SAP

Joshua Lane – Bank of America

David Lashway – Baker Mckenzie

Thomas Lind III – BlueVoyant

Shawn Lonergan – PricewaterhouseCoopers

Perry Menezes – KPMG

Clint Mixon – New York City Cyber Command

Erinmichelle Perri – The New York Times

Neal A. Pollard – UBS

Gregory Rattray – Next Peak‡

Michael S. Rogers – Former Director of the National Security Agency and U.S. Cyber Command

Katheryn Rosen – JPMorgan Chase

Monica Ruiz – Microsoft

Saleela Salahuddin – Facebook

Adam Segal – Council on Foreign Relations

Phil Venable – Google

Daniel Wallance – McKinsey & Company

Matthew Waxman – Columbia University

Evan Wolff – Crowell & Moring†

‡ Executive Director

† Co-Chairs



EXECUTIVE SUMMARY

The United States must reduce its vulnerability to strategic disruption by adversaries acting through cyberspace. Geopolitical and social forces, growing technological dependencies, and inherent advantages for ever more capable cyberattackers raise the risk of a major cyber crisis. Such a crisis could have significant adverse effects on public health and safety, the economy, and national security. Given mounting cyber challenges, the United States must take immediate steps to improve its cyber readiness to withstand such potential attacks.

In the spring of 2020, the School of International and Public Affairs (SIPA) reconvened the New York Cyber Task Force (NYCTF) to develop approaches to enhance cyber readiness through public-private operational collaboration that would enable more effective coordinated responses to cyber crises. The NYCTF assessed future risks to U.S. national security stemming from cyber challenges including political, economic, and technological developments; changing cyber conflict dynamics; and the COVID-19 pandemic. We then envisioned severe, yet plausible, scenarios projected for 2025 to examine how well the nation could defend itself in cyberspace. By looking to the future, the NYCTF shifted away from yesterday's issues to focus on longer-term enhanced cyber readiness. Our deliberations consistently identified shortfalls in our current operational collaboration capabilities and effective coordination efforts.

In this report, the NYCTF details recommendations to create an effective, whole-of-nation approach to enable enhanced cyber readiness through operational collaboration. At their core, these recommendations focus on establishing a public-private network of empowered nodes to provide effective crisis response to strategic cyber contingencies. The NYCTF sees the development of this network as a fundamental step in enhancing cyber readiness. We hope to build on the momentum created by the inclusion of key operational collaboration measures in the recent Solarium Commission Report and the 2021 National Defense Authorization Act (NDAA), as well as actions taken at the state and municipal levels and by the private sector. The United States must undertake a focused, urgent cyber readiness effort through improved operational collaboration now.

INTRODUCTION

The United States faces crucial cyber challenges as a nation. Our security and our economic and social life increasingly rely on the digital realm while adversaries seek to take advantage of such reliance. Enhancing readiness for effective national cyber defense must be a joint public-private endeavor.

Columbia University's School of International and Public Affairs (SIPA) has sponsored the New York Cyber Task Force (NYCTF), which convenes a cross section of leading members of business, policy, and academia to bring a unique perspective to cyber policy issues. In the fall of 2017, under the direction of Senior Research

Operational collaboration allows the private and public sectors to conduct coordinated cyber defense actions through highly synchronized operations.

Scholar Jason Healey, the NYCTF issued its first report, "Building a Defensible Cyberspace."¹ That report identified key leverage points — innovations across technology, operations, and policy—that grant the greatest advantage to cyber defenders over attackers at the least cost and greatest scale. Since its release, the report has helped focus government and industry efforts. The themes of this report were included in the U.S. Cyberspace Solarium Commission Report.² One critical leverage point identified by the first NYCTF report was the importance of "operational collaboration," the integrated public-private preparation and response to severe cyber crises. In the spring of 2020, the second NYCTF was formed under the direction of Adjunct Senior Research Scholar Gregory Rattray to build on the findings of the first report with a central focus on improving the nation's

ability to deal with severe cyber events by leveraging operational collaboration.

Operational collaboration entails deep organizational partnerships that enable coordinated responses to severely disruptive cyber crises. We envision these coordinated efforts at all levels of government—federal, state, municipal—in full partnership with the private sector. Enhancing national cyber readiness through improved operational collaboration has risen as a priority in cyber and national security dialogues, including in the recent Cyberspace Solarium Commission Report, the 2021 National Defense Authorization Act (NDAA),³ and the Aspen Cybersecurity Group's recommendations to the incoming Biden Administration.⁴ At its core, operational collaboration allows the private and public sectors to conduct coordinated cyber defense actions through highly synchronized planning and operations, as well as develop joint cyber capabilities to respond to adverse cyber events. Effective operational collaboration builds on previous progress in public-private information sharing by developing the necessary organizations, authorities, integration processes, and capabilities—across all levels of government and the private sector—to prepare for and respond to cyber crises.

The Task Force identified many challenges related to improving operational collaboration, the most pressing of which stemmed from a lack of established, exercised, and effective organizations to integrate public and private sector cybersecurity planning and response capabilities in a time of crisis.

U.S. adversaries will seek to take advantage of our nation's vulnerabilities in cyberspace. Our nation will live ever more deeply in the digital environment. The United States must prepare to meet future cyber readiness challenges today. This preparation must build on an under-

standing of the drivers of future cyber risks and recognize combinations of increasingly sophisticated adversary action, vulnerabilities created by our growing technology dependence, and weaknesses in our current response capabilities. Leaders must develop plans and capabilities to scale readiness to cyber incidents that materially threaten the United States. While developing more secure technology and systems is imperative, establishing effective cyber operational collaboration processes and effective cyber capabilities must be a national security priority. Effective future cyber readiness requires investing the resources to establish and strengthen public-private operational collaboration and the organizations, relationships, joint capabilities, and trust that is required. Accordingly, the NYCTF makes the following recommendations to establish enhanced cyber readiness in the United States:

The NYCTF acknowledges that much work has occurred to prepare the nation for cyberattacks. In the Federal government, these efforts must build on DHS Cybersecurity, as well as efforts of the Federal Bureau of Investigation, and in the private sector a rich array of Information Sharing and Analysis Organizations in key industries and providers of cyber response services also will provide strong foundations. However, the NYCTF assesses the nation's current capabilities do not amount to the integrated response network required to deal with the sophisticated cyberattack as posited in our scenarios. Our recommendations would subsume and build on the current patchwork of organizations to form a national structure for cyber readiness and response.

The views expressed herein are thought to reflect a broad consensus of the Task Force members, while individual views may differ, of course, on specific points.

- Recommendation 1**
Identify National Cyber Crisis Contingencies
- Recommendation 2**
Establish a National Cyber Response Network (NCRN)
- Recommendation 3**
Operation of the NCRN
- Recommendation 4**
Assess National Cyber Response Capabilities to Ensure Readiness
- Recommendation 5**
Ensure National Cyber Readiness through Training and Exercises

- Enabling Recommendation 1**
Establish Integrated Cyber Crisis Information Networks
- Enabling Recommendation 2**
Address Technology Evolution to Ensure Readiness
- Enabling Recommendation 3**
Remove Legal and Procedural Barriers to Enhance Response
- Enabling Recommendation 4**
Build Trust and Confidence for Cyber Crisis Response
- Enabling Recommendation 5**
Close Resource Gaps to Ensure Readiness

NYCTF ANALYTICAL APPROACH AND ACTIVITIES

The first New York Cyber Task Force looked at three levels of activity that provide defensive advantages to cyber defenders—policy, operational, and technological. This work focuses on the operational level—the level of activity where specific organizations conduct cyberattack and defense operations to achieve their objectives. The Task Force defines operational collaboration as the functional activities and actions that occur between organizations to achieve a mutually beneficial result. Applied to U.S. national cybersecurity challenges, organizations across all levels of government and the private sector must engage in operational collaboration. The relevant opera-

The Task Force chose to focus on political, economic, and technological factors and cyberattack and defense dynamics that might pose significant cyber challenges in five years' time.

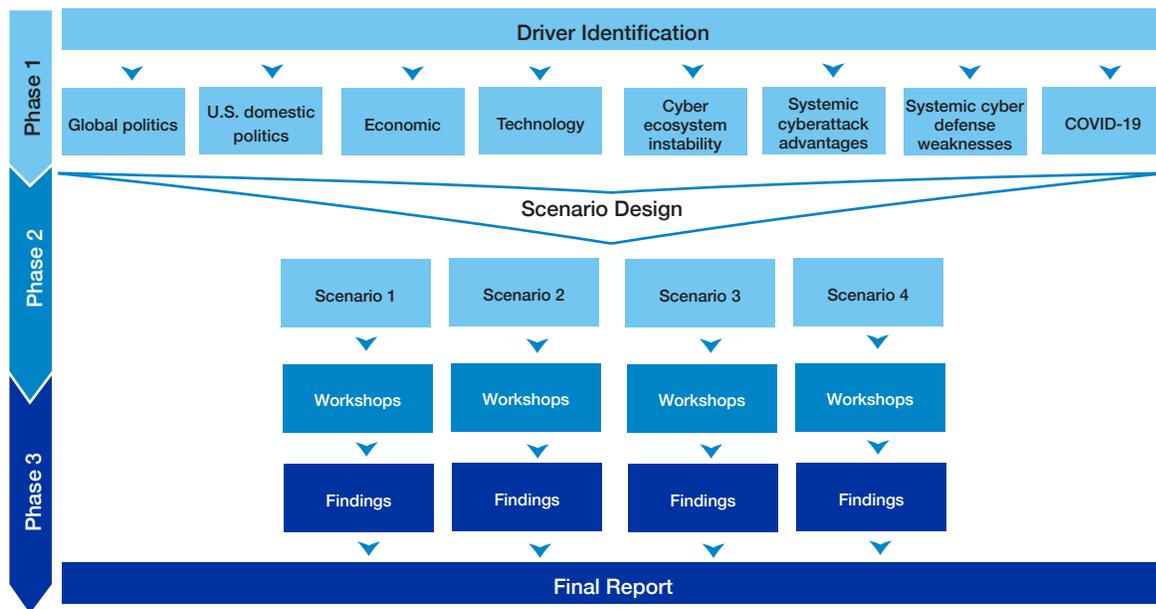
tional collaboration activities and measures required to enhance U.S. cyber readiness to prevent, address, and respond are the identification of national systemic cyber risks, identification of strategic adversaries, warning of systemic attacks, planning, preparations, and operations to respond in the case of cyberattacks that threaten national security. The Task Force chose to focus on political, economic, and technological factors and cyberattack and defense dynamics that might pose significant cyber challenges in five years' time. This focus on potential future risks instead of current problems provides insight on specific actions the nation can take now to enhance national cyber readiness for the future. The proposed approach to strengthen U.S. national security could serve as a model for other countries and has the potential to connect with systems of other countries to enhance global cyber resilience. We also chose to focus on challenges

posed by severely disruptive attacks rather than the conduct of cyber espionage.

This second iteration of the NYCTF joined forces with numerous organizations seeking to improve the nation's understanding and response to cyber challenges. We helped assess the Solarium Commission's work at their request, particularly their efforts around developing operational collaboration. The Task Force's report does not address all the recommendations in the Solarium Commission's report; however, the NYCTF report does recommend going deeper in key areas highlighted by the Commission Report. Specific Commission recommendations were mapped to corresponding scenarios in our workshops, and the NYCTF provided our findings to the Commission.⁵

Additionally, as the ongoing COVID-19 pandemic highlighted the necessity of cross-government collaboration for effective crisis response, the NYCTF sought an approach aimed at developing public-private operational collaboration at all levels of government—federal, state, and municipal. The Task Force teamed with R Street Institute in its ongoing work on state and local cyber response. NYC Cyber Command provided advice throughout this effort. We worked with the Atlantic Council in developing a scenario used in the NYCTF deliberations as well as serving as a scenario for the October 2020 Cyber 9/12 competition for future cyber policy makers.⁶ The Task Force also engaged leaders from a wide range of leading think tanks and industry associations, including the Aspen Cyber Institute, the Council on Foreign Relations, and World Economic Forum. Key private sector leaders across multiple sectors including finance, technology, media, and security as well as key private sector organizations, the Cyber Threat Alliance and the Analysis and Resilience Center were engaged. Task Force efforts have been enhanced and informed by these intellectual collaboration and ongoing participation in communicating Task Force findings.

Over the past year, the NYCTF conducted three phases of activity:



Our first step was identifying drivers of cyber challenges that may exist in 2025. Seven categories were examined: global politics, U.S. domestic politics, economic, technology, cyber ecosystem instability, systemic cyberattack advantages, and systemic cyber defense weaknesses. As COVID-19 took hold, an eighth category was identified to reflect the societal and technological challenges presented by the pandemic. Once categories were established, the group began to forecast specific potential future developments in each of the driver categories to form plausible cyber threat scenarios in 2025. The NYCTF believes the identification of these drivers provides a strong foundation for our nation’s understanding which cyber contingencies may prove challenging and how we must organize our operational collaboration efforts. We encourage readers to see Appendix 2 for our list of cyber challenge drivers. The Task Force made a deliberate choice to focus on challenges rather than on trends that might make cyber defense easier as it is easier to adapt to fortunate than unfortunate circumstances. In addition, the Task Force made a conscious decision not to address quantum computing in our work.⁷

Next, the Task Force designed a set of four scenarios that present a series of severe but plausible challenges

to national security. These scenarios covered a range of adversaries, potential attack vectors, and geo-political, economic, and technological factors that could combine to create very stressful cyber crises that might arise in 2025.⁸ This exercise was not an attempt to predict the future. However, the NYCTF leveraged deep expertise in considering the nature of scenarios worth further deliberation. Opinion can and will vary regarding the degree to which different drivers might come together and create a potentially severe cyber crisis. A multiplicity of potential toxic brews exists. The NYCTF believes that these scenarios serve as strong starting points to illuminate reasonable planning contingencies. We established the following four scenarios:

SCENARIO 1

Rising tensions in the Middle East lead to an increased U.S. presence in the region supporting Saudi Arabia and alarming Iran. The rapid integration of smart technology in U.S. critical infrastructure creates exploitable vulnerabilities. Iran uses these vulnerabilities to coerce the U.S. by targeting major metropolitan areas with disruptive attacks against the electrical and transportation sectors, causing intermittent power outages.

SCENARIO 2

China continues its rise as a competitive global player. China's rise as a global tech competitor enabled penetration of Internet of Things (IoT) devices and Artificial Intelligence (AI) databases, enabling for IoT- and AI based attacks on U.S. infrastructure in under-regulated critical industries. As tensions mount in the APAC region, China mounts a major disruptive attack against logistics, shipping, and healthcare, limiting the ability to marshal a response.

SCENARIO 3

North Korea, seeking to launder funds to enable nuclear weapons development, leans on cryptocurrency and cybercrime to funnel funds. As the digital underground thrives with North Korean sponsorship, criminal capabilities rapidly evolve. When tensions on the Korean peninsula eventually erupt, North Korea uses advanced cloud exploits to penetrate the financial system and wipe data, disrupting financial services. Attacks are amplified by cybercriminal actors using North Korean provided tools.

SCENARIO 4

As wealth disparities increase, driven by ever larger technology conglomerates, the nation moves to cloud-based, IoT-driven smart cities. Domestic political events and declining levels of public trust give rise to domestic extremist groups motivated by growing wealth divides. As public opinion drops to an all-time low, domestic extremist groups exploit the growth in IoT devices to launch amplified DDoS attacks, disrupting smart technology dependent emergency services and the media, causing disrupted responses and jammed lines of communication, while exasperating civil unrest with divisive messaging.

In the summer of 2020, the Task Force decided to adapt a scenario to focus on the possibility of domestic extremist groups conducting cyber disruption. Understanding how to reduce such risks must be included in national cyber defense planning. To conduct such planning, scenarios serve as guides, not predictions. The development and consideration of scenarios was viewed as a means to encourage the identification of potential cyber crises worthy of focused attention to assist in contingency planning efforts the NYCTF recommends. Detailed scenario descriptions are provided in Appendix 3.

Using the scenarios as starting points, we conducted workshops where Task Force members worked through the scenarios to identify the nature of operational collaboration activities that would be required, challenges to conducting these activities, and recommendations for overcoming those challenges. Each workshop had two phases. The first phase placed participants in the year 2025 during the crisis posed by a given scenario and focused on identifying likely gaps in our operational collaboration capabilities, processes, and organizations. The second phase brought participants back to the present to determine the short-term organizational and legislative actions necessary to enhance operational readiness for the future.⁹ In Appendix 4, we provide sets of challenges and findings that emerged in our workshop deliberations. The NYCTF believes using scenarios for a structured deliberation is one of the most effective ways to identify and understand the key operational collaboration challenges the U.S. must address. The NYCTF has synthesized our findings to focus on the most important drivers as a basis for making recommendations to enhance readiness for U.S. national cyber defense.

RECOMMENDATIONS TO ENHANCE NATIONAL CYBER RESPONSE READINESS

Effective national cyber crisis response requires a wide range of organizations to conduct complex technical and operational activities rapidly and in synchronized fashion across a variety of geographies and technical systems. Because the public and private sectors each have distinct comparative advantages in cyberspace, effective cyber crisis response will require both sectors to provide their unique capabilities. Thus, the nation's cyber readiness depends on the coordination of capabilities across the full spectrum of organizations at all levels of government and the private sector.

Effective national cyber crisis response requires a wide range of organizations to conduct complex technical and operational activities rapidly and in synchronized fashion across a variety of geographies and technical systems.

The NYCTF inherently views national cyber defense readiness as a whole-of-nation mission involving the private sector and all levels of government. As outlined below, much work needs to be done. Increasingly, in the digital realm, national security challenges and conflicts play out in networks and systems used and operated by the private sector. Our adversaries can reach down to the state and local level when seeking to conduct cyberattacks, as well as across multiple jurisdictions within the U.S. simultaneously. Many stakeholders across the nation will need to collaborate to enhance our nation's cyber readiness. Corporate and government leaders both must examine their risks and responsibilities to enable the investment of effort and resources the U.S. requires to enhance readiness for the challenges we have identified.

As others have considered U.S. cyber defense at the level of national security challenges, findings and recommendations—dating back to the 1998 President's Commission on Critical Infrastructure—focus dominantly on the role of the Federal government. The NYCTF certainly acknowledges the central role both the Executive Branch and the Congress will play. The NYCTF consciously decided not to analyze missions and recommend specific roles and responsibilities within the Federal Executive Branch. Instead, we focused on providing recommendations with a whole-of-nation perspective. The NYCTF does strongly support the establishment of a National Cyber Director and corresponding Office of the National Cyber Director (ONCD)—mandated in the 2021 National Defense Authorization Act—and we see the ONCD as the enabling organization for some of our recommendations.

The NYCTF further feels that state and local government leaders must also play key roles in responding to the types of contingencies we have identified that challenge the nation's security. Further, the private sector as the driver and supplier of technological foundations, as operator of critical systems and infrastructure, as the locus for attacks on national economic functions, and as providers of crucial cyber security response capabilities must be fully engaged. The NYCTF encourages private sector leadership focus on secure technological foundations and investing in cyber readiness capabilities to appropriately participate in the nation's defense. Our nation's security and future in cyberspace will require many to shoulder burdens and collaborate in order to reap the gains that the digital realm provides.

The NYCTF also recognizes that while we focused on U.S. national security challenges in the area of operational collaboration, we believe our recommendations must work within a global political, economic, and

technical environment. The NYCTF believes that collaborative efforts to achieve cyber security and resiliency must extend beyond national borders and hopes that U.S. efforts will contribute greatly in light of global challenges in this realm as well.

- Recommendation 1**
Identify National Cyber Crisis Contingencies
- Recommendation 2**
Establish a National Cyber Response Network (NCRN)
- Recommendation 3**
Operation of the NCRN
- Recommendation 4**
Assess National Cyber Response Capabilities to Ensure Readiness
- Recommendation 5**
Ensure National Cyber Readiness through Training and Exercises

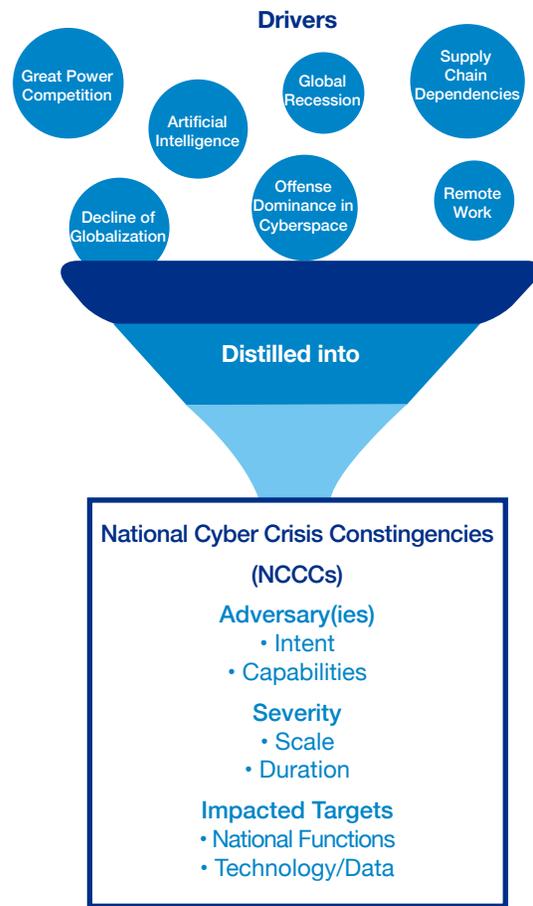
Recommendation 1: Identify National Cyber Crisis Contingencies

To assess our readiness, identify deficiencies, and recommend improvements, our nation must identify the key national security challenges that will confront our collaborative cyber defense effort. The NYCTF recommends that the Office of the National Cyber Director work with all stakeholders at Federal, state, and local levels and including the private sector to establish a program to identify a prioritized set of national cyber crisis contingencies (NCCCs) to:

- Guide selection of the organizations, communications, and responsibilities within the National Cyber Response Network (NCRN)
- Establish criteria for situational awareness by the NCRN in event of these NCCCs, based on potential impacts and risks, including the effect of an attack's scale, duration, and severity
- Focus of planning and exercise activities by the NCRN and the associated NCRN nodes leveraging public and private sources of information regarding adversary intentions and capabilities

- Provide criteria for assessing the readiness of the NCRN
- Establish a program to ensure the NCCCs are up to date and that findings from assessments are used to drive operational and budgeting priorities
- Provide the basis for exercises of the NCRN

Identifying National Cyber Crisis Contingencies



Organizations in the U.S. government already use scenarios to establish, exercise, and improve capabilities for national security challenges. Identifying NCCCs contributes to readiness by identifying strategic adversaries. The Department of Defense (DOD) uses scenarios based on the capabilities of both current and potential future adversaries and conflicts. The Federal Emergency Management Agency (FEMA) seeks to be ready to respond to a wide range of natural disasters. Neither DoD nor FEMA aims to predict the future. Both recognize that developing, exercising responses, and drawing les-

sions from plausible and challenging contingencies provide the intellectual preparation, the coordinated skills, and the improving capabilities to deal with the crises that will actually occur. National readiness is dependent on having established and assessed the capabilities to meet identified challenges. Sometimes, the nation is ready and responds well to these challenges. Other times, our national response capabilities are lacking. However, without systematically identifying the challenges and their scale, the nation will lack the drive to expend the time and treasure to establish capabilities and sustain them.

The U.S. has been fortunate to date and not surprisingly lacks experience in identifying the requirements and scaling operational cyber responses in the event of a severe cross-jurisdictional attack that impacts multiple organizations, national critical functions, and societal functions for extended periods of time. While forecasting the scale and depth of potential adversary actions is difficult, such an assessment is necessary in terms of planning national cyber responses and the requisite operational collaboration capabilities. Identifying a set of clearly defined NCCCs to scope the potential dimensions of a crisis allow us to assess the adequacy of current response capabilities; identify key conflicts that might arise; and estimate the level of capabilities, resources, and manpower necessary to draw the crisis to an acceptable close in a given timeframe. A program to identify NCCCs would codify this assessment and allow for planning processes to produce actionable findings for leaders to use in prioritizing operational and financial resources going forward.

The program to identify NCCCs will need to align with and provide input to numerous programs and planning constructs in the Federal government including DOD, the National Guard, DHS, the Intelligence Community, and others. The program must leverage knowledge and capabilities present in organizations such as the NSA Cybersecurity Directorate, DHS National Risk Management Center (NRMC), FEMA, and the private sector Analysis and Resilience Center (ARC), along with many others. State and municipal organizations such as state-level fusion centers and organizations like NYC Cyber Command must be involved. While analyzing specific intersections and process linkages required is beyond the scope of this NYCTF report, we recognize the complexity involved in establishing a whole-of-nation NCCC identification program.

We also recognize that publicly developed and widely shared NCCCs will pose challenges to traditional processes and boundaries regarding national security information and process. However, without active private sector involvement in the process and use of the NCCCs to guide establishment of response plans and capabilities, the U.S. will not be ready to defend itself in cyberspace. Neither the government nor the private sector can achieve their aims if they seek to conduct such an activity alone or leave the task to others to accomplish.

The NYCTF recognizes establishing the recommended program will take time, resources, and substantial commitment. Currently, analysis to guide the NCCCs will have to rely heavily on expert opinion. The NYCTF believes that the nation needs to work to establish

To assess our readiness, identify deficiencies, and recommend improvements, our nation must identify the key national security challenges that will confront our collaborative cyber defense effort.

modeling and simulation capabilities similar to those used to guide national response planning, including nuclear and conventional military conflicts, pandemics, and severe weather outbreaks. Appropriately identifying the contingencies that guide military, FEMA, and corporate planning exercises and capabilities assessment also require judgement and investment. The nation undertakes these efforts today to limit our risks. The U.S. must also do so as a whole-of-nation in the digital realm.

The scenarios used in the NYCTF workshops are not the most challenging possible types of disruptive cyberattacks that could be pursued by advanced adversaries facing the United States. Even so, we found operational collaboration capabilities sorely lacking across all levels of government and the private sector. The lack of foresight guiding current planning efforts as understood by the NYCTF was a recurring challenge throughout our scenarios. For example, Scenario One illuminated that the lack of informed planning will likely create challenges when mustering capabilities across just three municipalities, as stakeholders are not prepared to scale capabilities. The ONCD should use its authority to define,

evaluate, plan for, and prioritize key national cyber crisis contingencies. This effort must leverage resources across the government and the private sector to look forward in identifying emerging drivers and scale of cyber risks to the nation as our adversaries, technology, our economy, and society evolve. As recommended above, these national contingencies must drive requirements, capabilities, and assessments across all levels of government and the private sector.

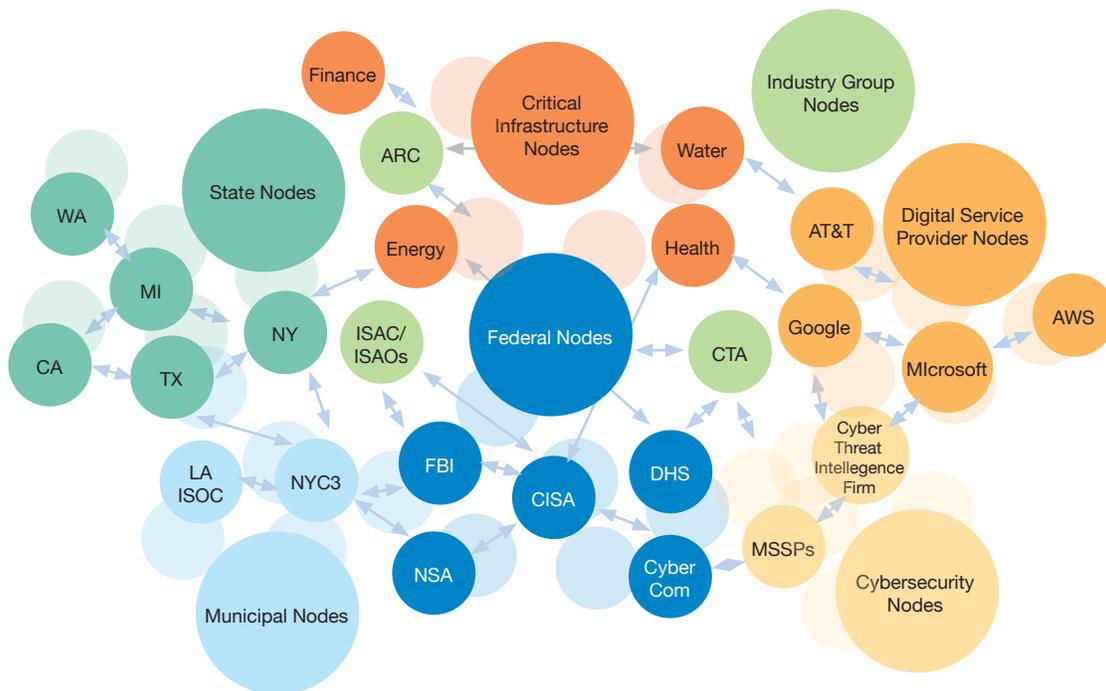
Recommendation 2: Establish a National Cyber Response Network

Our nation should approach cyber readiness through establishing a collaborative, coherent network leveraging existing information sharing and analysis organizations

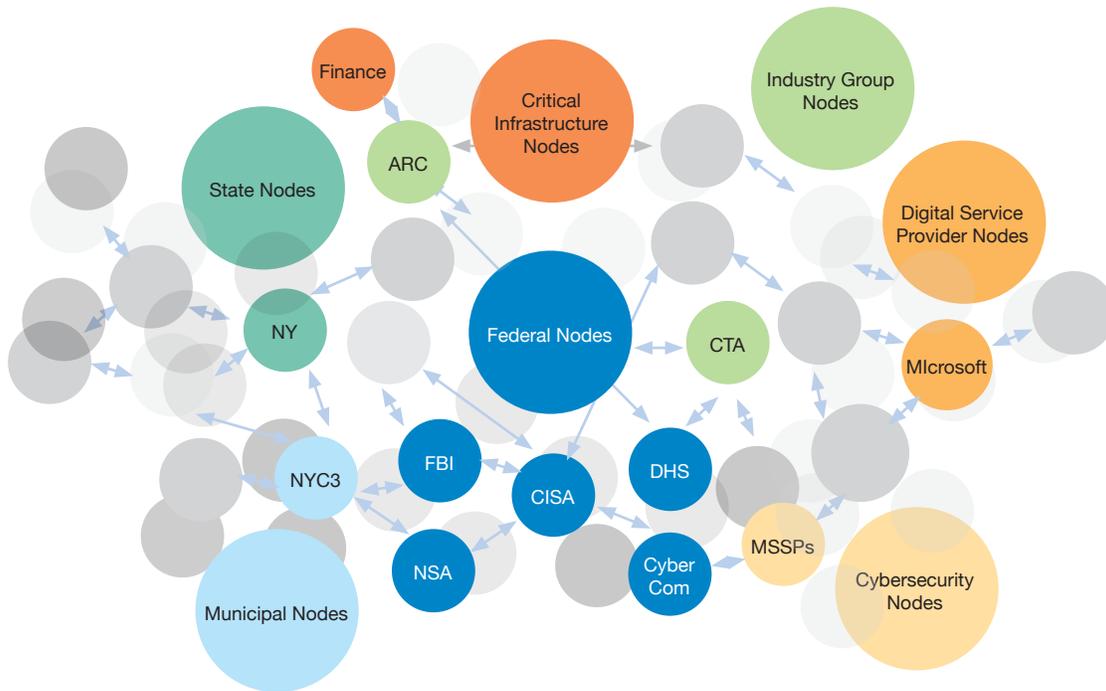
(ISAOs), network operations centers (NOCs), and cyber response teams in the government and the private sector, especially those response responsibilities for national critical functions. The NYCTF recommends the new National Cyber Director designate a Federal government agency to lead a national effort to establish a National Cyber Response Network (NCRN).

- The NCRN organizations would connect a wide range of existing and potentially new organizations across all levels of government and in collaboration with the private sector.
- The NCRN organizations must be empowered in advance to orchestrate specific response actions for cyber defense during severe cyberattacks.

National Cyber Response Network



Activated Nodes in a Crisis—an example based on NYCTF Scenario Three



The establishment of an NCRN is an important step, but authorities, responsibilities, and procedures must be established for dealing with attacks. The Task Force discussed how the continuing lack of a coherent approach to coordinating the array of public-private response capabilities has remained a recurring challenge. As a result, stakeholders affected by a major cyberattack on the U.S. as depicted in our scenarios would likely lack the ability to coordinate, communicate, and collaborate for an effective response. This challenge was illuminated in our workshop for Scenario Four. Task Force members doubted the ability for cross jurisdictional and private sector response teams to rapidly integrate and respond to disruptive attacks for the simple reason that current response teams are not designed or trained to do so. Task Force members also identified a similar integration challenge in their assessment that cities may not know how to properly use National Guard units deployed to help them in a crisis, due to a lack of knowledge of National Guard capabilities and organizational structure. For the capabilities and expertise of potential response forces, like the National Guard, to be deployed to the greatest advantage in a cyber crisis, these capabilities and integration process must be understood, mapped, and practiced well in advance. A widely accepted and inclusive National Cyber Response Network would be able to evaluate,

map, and coordinate Federal, state, local, and private response capabilities and could also serve as the hub for exercises and training. Routine exercises and training not only provide disparate response teams with a common understanding of what to do in a crisis; these activities can also serve as important relationship-building mechanisms and foster trust between teams.

The Task Force envisions an NCRN comprised of invited ISAOs, NOCs, cyber response teams, and related organizations from key private and public organizations able to collaboratively provide a collective NCCC response capability. Each organization in the network would provide cyber response capabilities based on its roles and mission within the government and private sector, combining with the expertise and talent to address different aspects of NCCCs. They would cooperate within the network using operational concepts and procedures established in collaboratively developed playbooks. This common operational language would extend the reach of the system, as a whole, across geographic jurisdictions as well as across critical sectors like electric power or core cloud services. In response to cyber crises, organizations in the network will have the legal and structural permissions to activate planned public-private partnered crisis response cells made up of law enforcement agencies,

digital services, cybersecurity providers, and representatives of national critical functions.

Types of organizations that would be part of the network include Federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and United States Cyber Command (CYBERCOM), state and municipal government agencies housing Cyber Response Teams (CRT), critical infrastructure information sharing and analysis centers (ISACs), as well as other industry associations and alliances with an operational focus. The network model will enable shared infrastructure, operational procedures, increased operational efficiency, and strategic dialogue between stakeholders. The Financial Services Information Sharing and Analysis Center (FS-ISAC) and Analysis and Resilience Center (ARC—formerly the FSARC) serve as two prominent examples of private sector capabilities that can engage the node network as critical hubs.¹⁰ The FS-ISAC aims to reduce cyber risk by serving as a hub for sharing cyber threat information and defensive best practices with global financial institutions, and ISACs exist across many industries as well as supporting state-level government. The ARC serves as an operational resiliency hub, conducting analysis of systemically important assets, providing warning of attacks on those assets, and developing resiliency measures. The private sector-led ARC collaborates with member companies, sector partners, and U.S. national security organizations. As private sector partners are identified and invited, similarly modeled organizations can be formed and integrated into the node network, improving public-private operational collaboration. The difference with today’s collaboration approach would be an expansion of this model into multiple other sectors, as well as the establishment of a common set of cyber crisis response capabilities and processes to enable effective integration in national security-level contingency response.

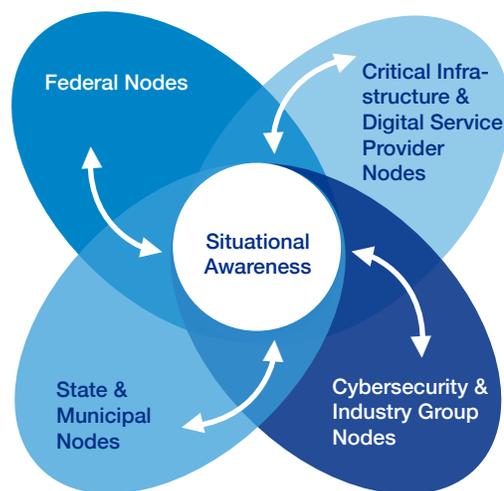
Recommendation 3: Operation of the NCRN

To leverage a collaborative NCRN, our nation must establish the capability to coordinate activity and share situational awareness among key governmental and private sector players engaged in national-level cyber crisis response.

- The federal lead agency would conduct overall coordination and enable readiness of designated NCRN nodes.

- The federal lead agency would establish a common concept of operations for the NCRN in consultation with operators of the designated NCRN nodes.
- The federal lead agency would enable situational awareness across the NCRN through establishment of a common operating picture for use during National Cyber Crisis Contingencies (NCCCcs). The common operating picture must be developed in consultation with operators of the designated NCRN nodes.
- Designated NCRN nodes would use the common concept of operations. These nodes would be responsible for developing the required integrative capabilities to leverage the common operating picture and participate in exercise and training to ensure readiness.

NCRN Operational Concept



Nodes feed:

- Attacks and Impacts
- Responder Status
- Current Actions
- Missions
- Objectives
- Desired State & Communications

Nodes receive:

- Intelligence
- Common Operating Picture
- Cyber Defense Actions
- Planned Proactive Defense Measures
- Desired State & Communications

Designated operational response teams will require a common concept of operations and operational picture for effective coordination. Creating a common operational picture that compiles and organizes information available regarding friendly and adversary status, activity,

and predicted actions for shared situational awareness is a fundamental necessity for crisis responders. An effective common operational picture must be ready and available before a crisis occurs. This picture must be continuously updated for the duration of the crisis response. Situational awareness enables warning of systemic cyberattacks and enables coordination of operations. This necessity was made evident in workshops on Scenario Three. Task Force members found that in the financial sector, institutions of different sizes and capabilities would likely have different views of what was happening in the situation, leading to differing, uncoordinated responses. Medium and small sized financial institutions would probably have little situational awareness due to differences in capabilities and posture. Managed Security Service Providers, the initial vector for the ransomware attack in this scenario, were expected to play a very limited role in response and remediation once the attack occurred, complicating response measures. Task Force members believed it likely that government response would not have the adequate authority, processes, or tools to coordinate these actors. More unified situational awareness through a standing coordinated set of data flows, information processes, and communications and display tools, often referred to as a common operating picture, can enable greater coordination of response capabilities. The designated federal lead agency would design a common operating picture process and supporting tools that participating partner nodes can contribute to as well as receive information from. The unified approach can be modeled on operational centers used to manage complex contingencies ranging from military operations and emergency responses to terrorist events and natural disasters.

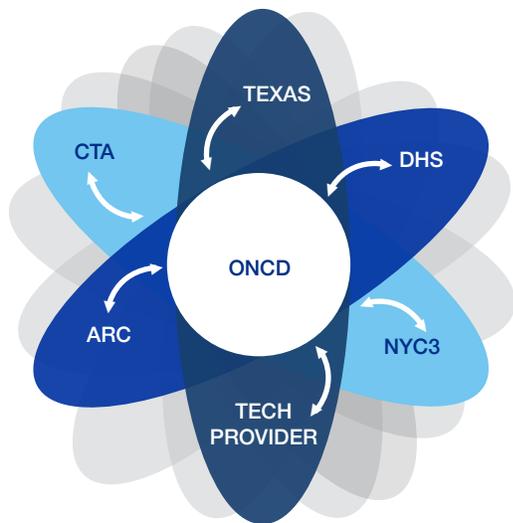
Recommendation 4: Assess National Cyber Response Capabilities to Ensure Readiness

The NYCTF believes the United States is insufficiently prepared for the types of contingencies considered in the scenarios. Assessing the readiness of U.S. cyber response capabilities is essential to guiding actions and investment. Assessment efforts should recognize both the challenges and the opportunities that stem from the distributed nature of U.S. capabilities that reside in many organizations in the private and public sectors. The NYCTF recommends the ONCD should be responsible for establishing a national cyber readiness framework in

collaboration with the participants in the NCRN. The NCRN will clearly outline the nature of cyber response capabilities necessary to respond effectively to the NCCCs, seeking to establish minimum requirements and identify capacity gaps across private and public stakeholders. The federal lead agency for the NCRN should use this framework to conduct annual assessments in conjunction with the designated nodes to assess readiness for the identified NCCCs. This cyber readiness framework should:

- Set standardized definitions for capabilities and resources
- Establish minimum readiness and capacity requirements for response to identified NCCCs
 - ◇ Minimum core capacity levels will account for the diversification of capabilities across jurisdictions and sectors
 - ◇ Readiness requirements should account for the possible need to leverage national organizations for high value/low density (HV/LD) assets that cannot be feasibly distributed across different levels of government and/or established within the private sector
 - ◇ Readiness requirement should include cyber training and exercise program participation by designated NCRN nodes responsible for collaborative response for those assets
 - ◇ The readiness and capacity requirements should be created in consultation with state, local, and private partners
- Enable shared understanding of necessary capabilities, facilitating investment decisions and expectations of deployment of key HV/LD capabilities across public and private sectors
- Direct ongoing capability and gap assessments for all participants in light of the NCCCs identified by the ONCD

Creating a National Cyber Readiness Framework



Nodes feed:

- Readiness Data
- Framework Feedback
- HV/LD Requirements

Nodes receive:

- Standardized Definitions
- Minimum Core Capacity
- HV/LD Construct
- Minimum Thresholds

Note: Recommended annual assessments will be self-conducted and signed off on by both the node being assessed and the designated lead agency aiding in the assessment.

The capability assessment framework should assess two categories: capabilities to integrate into the NCRN and operational response capabilities. Integrative capabilities are measured by the ability to coordinate with other response teams, i.e., the ability to support an organization under attack with additional capacity and integrate with a common operational picture. Operational response capabilities will be focused on local response capabilities necessary to assess, respond to, and recover from an attack, i.e., digital forensics, system and network rebuild, and administration. The cyber assessment framework must also map high value/low density (HV/LD) assets that are sustained by NCRN members with deeper resources and missions to provide these assets. The concept of HV/LD density assets underpins national security and emergency response operations in other realms. The nation can afford only a limited number of aircraft carriers, airborne command posts, or nuclear hazmat teams. In the cyber realm, response capabilities in limited supply would include personnel with advanced technical skill sets such as malware analysis and skilled personnel and infrastructure like deployable command centers that

can help local responders plug into the NCRN. Deeper understanding of the appropriate types and scale of national pools of cyber response HV/LD assets is needed. Conducting assessment across the NCRN regarding what can be done with local response capabilities and when and what augmentation might be necessary will help clarify HV/LD requirements. Having such a framework will also help clarify for cyber response coordinators at NCRN organizations what capabilities are at their disposal at any given point in time.

As discussed across all the scenarios, the nation lacks the capacity for assessing and coordinating the full range of public and private sector capabilities in the event of a multi-jurisdictional cyberattack. Creating an assessment framework enhances readiness by contributing to the planning and preparations necessary for effective response activity. In general, Task Force members agreed that most cyber response organizations do not feel individually responsible for assessing potential shortfalls in capabilities needed to address severe cyber crises. Establishing a common assessment framework of required cyber response capabilities is critical in effectively enhancing our operational cyber capacity. Without such an assessment framework, the nation will not be able to assess the maturity, depth, and adequacy of capabilities of response teams across private and public stakeholders. In the Scenario One workshop, participants were of the view that there are likely major differences in composition and strengths of different local, state, and federal response units as well as private sector response teams, especially across industries. For example, different National Guard units are likely to possess different cyber strengths, and the rail sector's response requirements and capabilities are likely to be different to that of the electricity sector. To account for these differences, the framework should define the capabilities of available response capabilities and measure that capability across government and private sector NCRN nodes to understand available expertise and capacity.

The NYCTF recommends that the newly established ONCD and designated federal lead agency for the NCRN design the assessment framework. The designated federal lead agency should work closely with each participant in the NCRN on tailored assessment criteria for that participant, according to the defined criteria across key NCCCs for a given NCRN node. The designated federal lead agency should also work with state and local governments to establish their frameworks, and work with providers of national critical functions and other

private sector entities through relevant ISAOs, ARCs, and other private sector nodes. Creating the assessments in consultation with the full set of NCRN organizations will enable the private sector to play a role in guiding appropriate capability requirements for investment rather than requirements established by Federal mandate, which might disincentivize participation. Task Force members assessed that this more inclusive co-creation process will simultaneously foster cooperation and trust between parties and aid stakeholder engagement in establishing the node network.

Recommendation 5: Ensure National Cyber Readiness through Training and Exercises

The United States needs to ensure the availability of the right skilled personnel and exercise its ability to respond to NCCCs in a vigorous, structured fashion to understand our readiness and potential weaknesses. The designated federal lead agency for the NCRN should cooperate with participants in the network to establish ongoing public-private training and exercise programs that will build proficiency in managing cyber crisis response operations. Exercises should be mapped to the NCCCs. The assigned federal lead agency should:

- Coordinate with NCRN participants in the conduct of an ongoing collaborative training and exercises program linked to key National Cyber Crisis Contingencies (NCCCs)
- Establish playbooks in consultation with the NCRN participants for national crisis response focused on the key NCCCs
- Over time, establish a national cyber training and exercise range to ensure command, control, and communications systems are adequately tested and functional in the case of a cyber crisis

Establishing collaborative training, exercises, and playbooks underpin an effective national cyber crisis response capability and contributes to readiness by enhancing preparation and planning. Without shoulder-to-shoulder training, drills, and exercises, operators will lack the familiarity of working together. While standardized playbooks and response plans are necessary for aligning operational teams, routinely practicing these response plans is critical to maintaining efficient response capabilities. The NYCTF assessed that the necessary level of collaborative training, exercising, and planning was largely ab-

sent across all the scenarios we considered. For example, in Scenario Three, Task Force members highlighted the existence of partnerships between the financial sector and key national security players in government as a positive indicator. However, as Task Force members explored the current partnership, major limitations became apparent. While these partnerships provide cooperation on information sharing and even collaborative attack warnings, potential mitigation measures are hamstrung by a lack of public-private response planning, exercises, and training. In the event of a major crisis, response teams from government and private sector stakeholders would likely spend critical time at the initial phase of a crisis integrating their processes, tools, and teams.

Regular collaborative training and exercises based on common playbooks involving NCRN teams would significantly reduce the time needed to integrate capabilities during an actual crisis. The federal lead agency can assist in coordination of regular large-scale exercises and training programs for multiple NDCN nodes. Exercises should include as many stakeholders as is feasible to help ensure that different nodes in the network understand the potential downstream effects if one sector comes under attack, while also learning how to provide support during such an event. Exercises should be mapped to the NCCCs. After-action reports and lessons-learned from collaborative training and exercises serve three important purposes. First, they identify shortcomings in the performance of the various organizations in the NCRN; second, they identify shortfalls in the overall performance of the NCRN due to unclear procedures, authorities, and responsibilities; third, they identify software and hardware shortfalls both within individual organizations and in the network as a whole that need to be upgraded. These observations can then be used to create and continuously enhance public-private response playbooks, supporting tools, and infrastructure. Establishing public-private training programs, exercises, and playbooks will increase the interoperability between stakeholders and response teams, enhance synergies in a time of crisis, and enhance trust and confidence between stakeholders.

The NYCTF believes the five recommendations detailed above can provide the foundation for U.S. national cyber readiness to deal with national security level challenges. All levels of government and the private sector must work together to establish these operational collaboration capabilities and defend the nation in a coordinated manner during a major cyber crisis.

ENABLING OPERATIONAL READINESS

During our deliberations, NYCTF members devoted significant time to discussing barriers that might impede effective operational collaboration. In many cases, challenges to achieving deeper operational collaboration have existed for an extended period such as establishing integrated information sharing to empower cyber incident response, legal and procedural barriers to sharing information, and mobilizing response resources as well as limited human and financial resources available to proactively enhance cyber response capabilities. In other situations, the NYCTF identified emerging challenges that may impede future operational collaboration including how new technologies may pose emerging vulnerabilities and risks as well as factors in our society between institutions. Additional challenges are contained in Appendix 4. Here the Task Force identifies five enabling recommendations that the NYCTF believes will have the greatest positive impact.

Enabling Recommendation 1
Establish Integrated Cyber Crisis Information Networks

Enabling Recommendation 2
Address Technology Evolution to Ensure Readiness

Enabling Recommendation 3
Remove Legal and Procedural Barriers to Enhance Response

Enabling Recommendation 4
Build Trust and Confidence for Cyber Crisis Response

Enabling Recommendation 5
Close Resource Gaps to Ensure Readiness

Enabling Recommendation 1: Establish Integrated Cyber Crisis Information Networks

The United States must work to ensure that cyber responders can leverage a robust range of information and knowledge across the diverse ecosystem of organizations and perspectives that will make up the NCRN. The designated federal lead agency leading the National Cyber Response Network (NCRN) should collaborate with operators of the designated nodes to establish national integrated information streams orchestrated to collect and disseminate key information between NCRN organizations to better prepare and respond.

- Organizations in the network collect data drawn from threat intelligence, contingency planning, and exercises seeking to integrate findings into future response plans and response maps as well as provide warning and enable coordinated response
- Organizations in the network identify best responses to different categories of attack and disseminate findings to other nodes

Effective information sharing, shared intelligence, and collective warning between the full spectrum of stakeholders is critical for a coordinated cyber response. These efforts have been a major area of focus for CISA, which, for example, has established the Cyber Information Sharing and Collaboration Program as well as the Information Sharing and Analysis Organizations; however, these organizations have not nourished the level of operational information sharing required for public-private response at a scale to effectively coordinate response during a major cyber crisis.

National cyber readiness efforts must now go further. A lack of integrated information sharing streams will likely result in a disorganized cyber response effort by

the many parties involved. This challenge was faced in Scenario Three, where the working group found that financial sector companies might be unprepared for adversary responses to escalation, as they are unlikely to be informed of possible U.S. cyber counter actions designed to disrupt adversaries. Throughout our workshops, NYCTF members highlighted the types of information that would likely be missing. Efforts outlined in Recommendation Three on situational awareness displayed the need for shared information regarding status of friendly response capabilities, adversary activity, and information on current and planned friendly actions.

Effective processes for deep public-private intelligence sharing and operational coordination are still in nascent stages even where mature private sector capabilities exist. The Pathfinder initiative discussed in the Solarium Commission provides an example of current efforts to improve public-private shared intelligence sharing and warning.¹¹ While the program is a positive step for operational collaboration, in order to increase public-private coordination, the nation must move beyond asynchronous threat information sharing to fully enabled real-time shoulder-to-shoulder collaboration for intelligence analysis and attack warning. Similarly, all participants in the NCRN must view impacts of attacks in a similar fashion, for example in the case of disruptive attacks against an organization that are causing systemic technological or economic effects.

The NYCTF faced challenges in Scenario Four when considering the ramifications of an advanced domestic extremist group attacking central nodes in smart city networks. We found that response teams would likely have little clarity on each other's actions and limited ability to share information about projected actions with each other. Integrated information networks need to be created to share cyber response and adversarial information between responders. Cybersecurity information sharing is particularly challenging because private sector networks are often the frontline for cyberattacks requiring rapid information from the intelligence community and other sensitive government sources. The need for shoulder-to-shoulder collaboration and rapid sharing of sensitive information is in this regard unlike the traditional approaches we have used in public-private collaboration for national security.

Collaborating responders can greatly enhance readiness

by sharing risks and impact assessments across sectors and with different levels of government while providing status of response capabilities. Threat information enhances coordination by providing intelligence on adversary capabilities and intent and can provide warnings around current and predicted adversarial actions. Sharing information across sectors can help defenders understand and plan for risks and impacts outside their own sectors. For example, if the electric grid is targeted, potentially impacted government and private sector organizations can plan for outages. Integrated information streams can be managed through the NCRN common operating picture, enabling designated nodes to partake in the sharing and dissemination of information.

Enabling Recommendation 2: Address Technology Evolution to Ensure Readiness

The NYCTF analysis of drivers for national security emerging for the U.S. in cyberspace continuously returned to the challenge of the speed of technology changes, complexities such change causes for seeking collaboration, and coordination in response to cyberattacks. The NYCTF recommends national efforts should seek to engage and enable leading private sector technology firms and organizations, in addition to private-held national critical functions providers, in cloud computing services, Internet of Things (IoT), and artificial intelligence (AI) to develop the capabilities to engage in the establishment of the NCCs and participate in the National Cyber Response Network (NCRN).

- Designate large-scale cloud computing services as critical national assets, and define a collaborative approach for cyber response for National Cyber Crisis Contingencies (NCCCs) that involve private sector cloud operators. This effort will aim to:
 - ◇ Increase collaboration between the government and private sector necessary to understand the readiness of core technology infrastructure and services
 - ◇ Seek to establish a private sector-led systemic cyber analysis and resiliency organization with the capability to participate in the NCRN as a dedicated hub in the operational response network

- Incentivize leading IoT technology firms to establish a private sector–led systemic cyber analysis and resiliency organization with the capability to participate in the NCRN. The established IoT resiliency hub should focus on:
 - ◇ Developing capabilities for crisis reporting and impact assessment to discover supply chain vulnerabilities and seek to avoid surprises regarding risk exposure during a crisis
 - ◇ Establishing private sector lead standards for security design and testing of IoT devices
- Establish industry-driven operational resiliency and cyber contingency planning hub for leading AI organizations, focused on proactively identifying data integrity challenges and orchestrating response as part of the NCRN
 - ◇ Plan for data integrity challenges by developing improved technology and implementable integrity checks to respond at machine speed
 - ◇ Design AI-specific operational response standards and playbooks in case of AI-based attacks

Cloud Technology

The Task Force sees the rapidly growing adoption of cloud technology by a wide and increasingly critical range of business and public services as both a vulnerability and an asset. The increased uptake of cloud services among a limited number of major providers constitutes a high-value target for cyberattacks. The lasting effects of COVID-19 amplify the danger as private companies and government organizations leverage the technology with the widespread adoption of remote services. Task Force members' primary concern was the unclear and unmapped risk landscape created by transitioning to cloud-based hosting and services, encountering the issues raised by major cloud adoption in Scenarios Three and Four. Posited attacks on the financial sector exploited cloud-based services to spread rapidly through financial institutions, crippling the nation's access to critical financial services. Similarly, in Scenario Four, domestic extremist groups targeted cloud-based services as cloud had become integral to the functionality of cities, cre-

ating a locus of vulnerabilities as new technologies were integrated. However, we quickly identified that centralizing the continued mapping of new dependencies, vulnerabilities, and risks based on increased use of cloud technology would prove monumental and infeasible. Instead, the U.S. must ensure that individual enterprises moving to the cloud have the capability for improved dependency analysis, risk management, and resiliency practices. These practices must explicitly include and seek to leverage response capabilities in the advent of major cyber crisis contingencies. Key cloud providers should be included as a critical node in the NCRN as an essential element of the nation's networking and communications infrastructure.

Task Force members were also concerned that a lack of a defined government role would lead to a lack of contingency planning and readiness for cyber crisis contingencies that involve cloud-based attacks. Public and private response coordinators will need to determine their respective roles and responsibilities when cloud services are involved and how they will cooperate while attempting to respond to the crisis. The nation needs to understand the wide and potentially severe impacts that outages of a major cloud provider can cause across multiple sectors of economic and governmental activity. As cloud service providers become part of the NCRN, this situational awareness will need to be provided to the network as a whole. Numerous decision points will include deciding on the degree to which digital forensics are shared; coordinating operational response teams with response teams from private sector cloud partners; and deciding when a digital environment is sanitized and can be safely put back into operation. Playbooks to provide guidance for many of these decisions can be developed in advance when time pressures are not present. This challenge arose in Scenario Three, with Task Force members highlighting likely challenges in defining the respective roles between cloud service providers and government response elements. The lack of cloud service providers' integration into the national cyber response ecosystem will likely cause an overall lack of contingency planning for cloud vulnerabilities. As the cloud continues to become an important component of our nation's infrastructure, the NYCTF believes that the nation must establish strong operational collaboration mechanisms with major cloud providers as a critical national asset and engage cloud stakeholders in a similar model to what currently exists

for the telecommunications sector.¹² Further, seeking self-organization by the key industry players of a cloud services provider analysis and resiliency center would be a major step forward, enhancing the ability of cloud service providers to establish standards and interoperability, while preserving continued independence.

The Internet of Things

IoT presents vast technological opportunities across the full spectrum of economic activity. IoT is expanding its presence in operational technologies (OTs), becoming integral in manufacturing and delivery of industrial production, and embedded in critical infrastructure and homes through smart cities, ports, and power grids. However, IoT devices suffer from the common challenge of creating operational, commercially viable products quickly without the application of effective security practices. Efficiency and speed to market is often prioritized over security, causing an already immature IoT security environment to increase risks further. However,



IoT devices suffer from the common challenge of creating operational, commercially viable products quickly without the application of effective security practices.

the lack of response readiness is our primary concern. We encountered these challenges in Scenarios Two and Four, with IoT becoming a primary attack vector due to unexpected vulnerabilities. In Scenario Two, the rapid pace of adoption caused an oversight in supply chain risk. This vulnerability led to a severe cyberattack enabled by an adversary placing malware in a software update to IoT devices. As described in Scenario Four, smart city technology integrating IoT devices could enable domestic extremist groups with opportunities such as creating vast botnets from the rapid growth in new devices. Finding the balance between rapid deployment of IoT capabilities while maintaining security is critical to enable cyber resiliency. The formation of a private sector–led systemic cyber analysis and resiliency organization focused on IoT providers and services has the potential to increase the sector’s resiliency by providing access to the NCRN’s response capabilities, while improving public-private

collaboration. Participation by the IoT industry in the NCRN will allow NCRN participants to collaborate on key issues, such as what the relative roles are of ISPs versus device manufacturers in remediating IoT attacks.

Artificial Intelligence (AI)

The NYCTF faced similar challenges when planning for how AI will impact our nation’s cybersecurity. AI, like IoT and cloud technology, has been rapidly adopted across industries. The nation is witnessing the integration of AI in finance, e-commerce, management functions, manufacturing optimization, even in data modeling for healthcare as the nation combats the COVID-19 pandemic. AI brings a different set of risks requiring cyber contingency planning and response. Because AI is highly dependent on the integrity of data used in training AI systems, protecting that data from unwanted exposure is critical. By altering or poisoning data, AI systems can fail in unforeseen ways such as altering predictions or misclassifying people or images. The approaches for detection and remediation of data alteration are immature. The Task Force faced this challenge in Scenario Two as a new, more virulent type of coronavirus emerged, adversaries altered data sets, compromising the ability of the medical industry to model the virus spread properly. Creating resiliency for data sources and protecting data integrity is a crucial step in securing AI vulnerabilities. Attacks on AI data streams, databases, and data backups will require dedicated contingency plans and response playbooks. For these measures to succeed, the U.S. will need private sector leadership in helping to co-develop resiliency and response capabilities for the AI sector. Incentivizing current industry leaders to establish an organization to serve as a designated NCRN node would be a progressive step in establishing public-private resiliency planning for AI systems. AI sector participation in the NCRN will allow the NCRN to integrate key capabilities like automated threat recognition and system response.

Enabling Recommendation 3: Remove Legal and Procedural Barriers to Enhance Response

The NYCTF found that despite ongoing attention in past studies regarding how existing laws, regulation, and proscribed processes negatively impact private-public

operational collaboration, these barriers remain high. Additionally, the lack of clarity of existing laws, regulation, and procedure can paralyze action in the case of a cyber crisis. The nation needs to continue proactively clarifying authorities and establish appropriate agreements to remove legal concerns hindering effective public-private response in times of crisis.

- Build on the 2015 Cybersecurity Information Sharing Act, which successfully focused on general enablement of ongoing threat information sharing rather than deeper, more sensitive sharing and integrated public-private information flows needed for cyber crisis contingency response planning and action. All stakeholders require proper authority to exchange necessary and appropriate information with national critical function operators and other public-private partners in the event of NCCCs. Key actions would include:
 - ◇ Establishing a framework to address legal and procedural barriers for providing NCRN participants in emergency situations access to appropriate information
 - ◇ Creating situational and jurisdiction-dependent communication and resource procedures between private sector, state, and local organizations to enable states to work more effectively with local law enforcement and private enterprises, and to empower states as a key element to coordinate operational response in the node network
- Provide legal and procedural incentives and clarifications for private sector stakeholders to engage with the NCRN
 - ◇ Normalize emergency collaboration clauses in public-private contracts to enable integration of private partners into cyber crisis response; for instance, agreement on the development of emergency clauses should be undertaken that by default offer full protection from legal recourse for any information appropriately disclosed to better enable a timely response to a declared NCCC
- Decrease barriers for companies to participate in information transfer by assuaging concerns of compa-

nies operating globally that information sharing will impact business processes or reputation. New measures must not be seen as globally adversarial or violate international law by clearly defining information types to be shared and fit within constructs such as the EU General Data Protection Regulation

At all levels, legal and procedural barriers often hinder the ability to muster and coordinate public-private response teams quickly. Non-disclosure agreements, legal clauses within contracts, and other mechanisms consistently threatened to block an expedient response as liability concerns over actions that responders might undertake could be construed after the event as causing vulnerability, disruption, or damage. Liability concerns must be clarified in advance. Such concerns often hinder efforts to retrieve valuable digital forensics data and onboard private sector capacity to response teams during a crisis. Legal and procedural barriers barring private sector aid in Scenario One, where municipal governments had contracts with private sector vendors, were identified as a highly problematic issue. The lack of agreed mechanisms in place could slow down the formation of public-private response, causing responders to spend valuable time making legal arrangements rather than having them in place beforehand. Such mechanisms must be in place to enhance the smooth integration of private stakeholders into the response if defenders are to leverage all the capabilities at our disposal effectively. A natural place for legal and procedural mechanisms to be orchestrated is by the NCRN nodes. By having existing private sector nodes with pre-cleared collaborative response cells within the network, the full spectrum of public-private response capabilities will stand ready to respond.

Barriers also limit the ability to share information, both with private sector stakeholders and across different jurisdictions. Municipal and state-level governments, particularly law enforcement, often do not possess the proper authorities to access federal-level intelligence and other information necessary to achieve common situational awareness. This same issue extends to information sharing with the private sector. Such impediments have long been identified as problematic; however, efforts to address necessary changes to policy, law, regulatory guidance, and other governmental instructions have made limited progress. The 2015 Cyber Information Sharing Act spurred progress, successfully lowering many barri-

ers to information sharing. However, stakeholders have rapidly come to realize the limited value of high volumes of tactical threat intelligence, like indicators of compromise, especially for organizations lacking sophisticated or well-integrated threat intelligence and security operations teams. The NCRN can help rectify this issue by proactively establishing a level of trusted access to information into the nationally validated network, fostering adoption of an integrated information flow and a common operational picture.

Legal mechanisms must be in place to enhance the smooth integration of private stakeholders into the response if defenders are to leverage all the capabilities at our disposal effectively.

Overly prescriptive cyber-related regulation was also predicted to cause serious operational collaboration challenges. Overregulation creates the possibility that regulated parties will focus on avoiding liability and even preemptively outsource key security functions, resulting in a checkbox mentality toward security regulation rather than proactive mitigation of the highest security risks. In Scenario Three, the possibility of an overregulated financial sector turning to MSSPs to meet requirements for appropriate detection and response capabilities raised concerns over concentration risk where multiple institutions could be targeted through a single exploit in an MSSP. Empowering private sector hubs to partake in operational collaboration through the NCRN can help direct resources to systemic risks and build national cyber resiliency instead of low-value check list compliance activities. We believe that there are significant opportunities to strengthen the national cyber response system as a whole by providing increased visibility for private and public stakeholders into each other's concerns, possible response plans, and capabilities.

Another significant challenge stems from the fact that sectors with inadequate cyber security and resiliency standards are likely to not have the correct incentive structure to invest in resiliency measures. In Scenario Two, Task Force members identified this concern as the logistics and shipping sectors suffered disruptive attacks. The logistics and shipping sectors were felt to have lower

security standards for supply chain sourcing due to the global characteristics of their business. To counter this risk, policy makers should collaborate with the private sector to incentivize creation of sufficient resiliency measures where regulation may prove insufficient but which can have critical second-order impacts on U.S. national security. The Task Force felt that industry-driven standards development enforced in the courts would provide the most efficient path forward. Experience with the National Institute of Standards (NIST) and Technology Cybersecurity Framework provides a good example of where collaborative effort between the government and private sector can create the basis of reasonable expectation for cybersecurity due diligence and accountability for organizations. Further, integration of response nodes for such sectors in the NCRN can help ensure proactive public-private operational collaboration participation in case of severe disruptive attacks. Through more vigorous national exercises, particular legal and procedural barriers can be identified, and specific barriers can be removed or refined.

Enabling Recommendation 4: Build Trust and Confidence for Cyber Crisis Response

In order to effectively collaborate in cyber response, a wide range of organizations will need to trust each other and the information streams and situational awareness they will share. The nation needs to establish widely accepted trusted sources of information and analysis regarding cyberattacks, the attackers, and the impacts on targeted organizations, sectors, and society, within public-private operational constructs. Specific steps recommended by the NYCTF include:

- Encourage and enable the private sector and different levels of government to have liaisons, secondments, and alternative programs to exchange personnel to improve collaboration processes and build trust between organizations
- Encourage cybersecurity officials to cultivate relationships with traditional media organizations and reporters to build trust, and ensure that accurate, substantive feeds of relevant information have a channel to the public domain
 - ◇ Increase access for observers from media and public-interest groups to NCRN operations as appropriate to enhance public transparency into cyber activity

- Co-design, with public and private stakeholders, improved digital literacy programming to educate on understanding what constitutes misinformation during a cyber crisis, how to distinguish factual reporting from disinformation related to cyber events, and how to report misinformation to help enable platform managers to take down inappropriate content
 - ◇ Create mechanisms for the public to flag and report disinformation during a cyber crisis event for vetting by communication platform managers
 - ◇ Increase collaboration between governmental communications, traditional media, social media platforms and influencers through crisis co-creation of cyber crisis communications playbooks for media stakeholders and NCRN node operators
- In moments of cyber crisis ripe for disinformation campaigns, ensure that the government and media companies have appropriate active collaborative mechanisms to moderate content with stricter fact-checking, publishing criteria, and warnings of misinformation campaigns when they occur

Trusted Information Sources

The NYCTF believes that building trust is a necessary step in realizing cyber operational collaboration and readiness. The wide range of cyber crisis responders and stakeholders cannot work together in a crisis in the absence of trust in each other. Recent events provide both positive and negative indicators for trust and confidence building. The efforts that combined activities of the Department of Homeland Security and the Cybersecurity and Infrastructure Agency (CISA) with actions such as the TrickBot takedown helped secure the 2020 election.¹³ These actions undertaken with high levels of transparency and public announcements that rectified misinformation provide a positive model. As we deliberated on these issues, we distilled the trust problems to three primary challenges: establishing widely accepted, trusted sources of information and analysis regarding cyberattacks; attaining trust between the government at all levels and media organizations; and countering mis-

information in order to facilitate the public's trust and confidence in response to cyber crisis situations.

Cyber responders lack the ability to get trusted high-quality information regarding impacts of attacks and public reactions. The media plays a crucial role but lacks deep cyber expertise and trusted sources. Also, the NYCTF questioned whether cyber crisis responders would trust sources if media and other communications systems were compromised by misinformation or deliberate deception. We found ourselves challenged by limits to trust in Scenario Four, which focused on domestic extremism. We assessed that if media sources were struck by major misinformation campaigns and local governments were crippled by cyberattacks, the ability for responders to gain a clear situational picture of events would likely be hampered. The lack of accurate information was caused by a lack of trusted sources, particularly due to cybersecurity's lack of an equivalent tracking organization such as the Food and Drug Administration (FDA) or Centers for Disease Control (CDC). Progress has been made by CISA in acting as a coordinating agency; however, CISA was not designed to take on this role at the pace and scale of the cyber crisis posed in our scenario. The nation lacks an organizational structure capable of coordinating and tracking information related to cyberattacks, which creates disjointed and differing narratives from sources on the ground, likely creating pools of conflicting information. Simultaneously, this gap fails to integrate private and public information sources into a consolidated stream. This deficit will make establishing the necessary common operating picture more difficult. The necessity of creating a trusted and resilient information monitoring and dissemination capability can play an integral role within the NCRN described above.

Strengthening trust between all levels of the government and media organizations is also a challenge. Organizations with low trust quotients in each other often have unclear cooperation mechanisms. A prominent example of these potential challenges to trust arose in Scenario Three between the financial sector and regulators. Task Force members assessed that financial sector organizations would likely be hesitant to work alongside the same bodies that regulate them, concerned they might expose themselves to regulatory measures. While proactive filtering of information is potentially useful in understanding attacks and orchestrating response, such unilateral filtering regarding potential systemic impacts of cyber-

attacks could potentially lead to regulator reaction and even punishment.

Building trust is a necessary step in realizing cyber operational collaboration and readiness.

Trust issues related to competing priorities were significant in the media's case in reporting on digital public safety. Public distrust of media, as well as government actions and corporations, are likely to continue to grow, with significant portions of the population believing that the media, as well as other actors, have political and commercial motivations for their messaging. This type of problem arose in our workshop deliberations around Scenario Two. Participants felt the logistics sector will be unlikely to trust government responses enough to be forthcoming in disclosures about attacks and impacts for fear of encouraging stronger regulation and generating liability. Alternatively, public sector response teams are likely to view the relevant private sector stakeholders as incapable due to the perceived lack of security and resiliency measures. For these reasons and others, actionable measures to enhance transparency are required. Integrating private stakeholders within the node network is one measure to help organizations build trust with each other. Participants in the NCRN should enable media access as appropriate to promote public transparency. A far-reaching idea would be to consider embedded reporters in times of cyber crisis, similar in fashion to war correspondents. Establishing procedures for ensuring the correct reporters are provided access and the nature of information reported would be challenging but precedents exist and should be explored.

Countering Misinformation

Challenges that arise concerning trust and confidence cannot discount the rampant phenomenon of misinformation. The potential for misinformation to dominate media cycles already constitutes a high risk to political stability around the globe. The ramifications of a well-timed disinformation campaign in conjunction with a significant cyberattack pose major risks to exacerbating impacts and impeding responses in a NCCC. The problem challenged the Task Force, particularly in envisaging responses in Scenario Four, as crisis responders and the

government would have wanted to attempt to provide information on ongoing events to the public. In that scenario, for example, the workshop participants noted that false reports of failed government responses could have led to increased chaos and disruption, as extremists could be emboldened and responders not aware of the true state of events. Challenges in holding media, broadly defined, to an appropriate standard for validating information before publishing content only heightens these concerns. The challenges highlight the need for a multifront initiative to counter disinformation. All stakeholders in effective national cyber response must take responsibility for educating the public regarding how to judge what information is trustworthy. Making progress in building general digital literacy presents a formidable, yet essential, challenge at the national level. Such initiatives focused in the area of cyber crisis response will require thoughtful design of public education programs and campaigns, working alongside media and private stakeholders to build advocacy as well as resourcing from all levels of government.

Enabling Recommendation 5: Close Resource Gaps to Ensure Readiness

The nation must invest deeply if the capabilities outlined above are to exist. These investments should come from both public and private sectors. The U.S. government should work to establish a well-funded national program for enhanced cyber response capabilities across all levels of government and the private sector. This program must be considered a national defense priority.

- The national program must ensure the establishment of the National Cyber Response Network (NCRN) with the associated capabilities described above as well as fund necessary Federally provisioned high value/low density (HV/LD) cyber crisis response assets.
- The program must effectively integrate the full range of existing organizations. Further, organizations will require additional resources to fully meet the requirements driven by adequately addressing the NCCCs
- A Cyber Response and Recovery Fund must be established to support sustained funding of cyber response operations. This fund should be separate from funds dedicated to natural disasters or health crises.

The NYCTF identified the need for two types of cyber response capabilities investments: long-term proactive

capacity building and dedicated cyber emergency funding. For proactive operational investments, a national capability threshold must be designated by cyber coordinators to establish a minimum level of resources required based on the previously discussed set of National Cyber Crisis Contingencies (NCCCs). For example, does the nation need to be ready to defend three metropolitan areas at once, or five? Against how many simultaneous types of disruption? What level of capacity fulfills that need? Threshold definition must consider and involve private sector stakeholders. As the NYCTF detailed in the scenarios we developed, private sector organizations and functions are often primary targets. If cyber crisis resiliency thresholds are created without inputs from the private sector on requirements, the defined thresholds will lack buy-in from the stakeholders who will have to make the resiliency investments. Further, assets required by each stakeholder will need to be mapped. Mapping must take into consideration the size and resources of the relevant stakeholder; national security planners examining NCCCs cannot expect San Angelo to sustain the same level of capabilities as Houston. A community credit union will undertake different resiliency planning

for a much different role than a globally, systemically important bank. The Federal lead agency must also identify which assets will be provided by the national level, and which public and private stakeholders might require rapid deployment of HV/LD assets in the event of which sorts of crises.

Emergency funding emerged as an issue as Task Force members raised concerns over the endurance and scalability of responders in the case of a major cyber crisis. In our first scenario workshop, Task Force members vocalized concerns over the ability to maintain response teams, especially private sector teams, if funding and resources ran out. The severity of risks posited by the NCCCs will require that response teams and associated support capabilities not rely on volunteer assets, requiring plans and resources for sustained operations which currently do not exist. Establishing a Cyber Response and Recovery Fund, as recommended by the Solarium Commission, to support sustained funding of cyber response operations would help address this problem.



CONCLUSION

The United States faces growing challenges in cyberspace that pose fundamental national security challenges. The nation is not ready. The private and public sectors must collaborate in order to meet the challenges. As a first step, the NYCTF recommends the Federal government must clearly establish responsibilities under the newly appointed National Cyber Director for national readiness for severe cyberattacks. All levels of government and the private sector together must establish processes for cyber crisis contingency identification and prioritization to guide much deeper programmatic operational collaboration investments to enable public-private response capabilities to deal with these contingencies.

Even in these challenging times, the New York Cyber Task Force has offered a number of specific recommen-

dations. We urge the Biden Administration working with Congress, state and local governments, and U.S. business leadership to make this investment a priority.

Strengthening national cyber readiness should be seen as an opportunity, not a burden. Cyber readiness in the face of severe but plausible cyber shocks will enable confidence in the digital transformations already underway. The campaign to defeat the coronavirus has taught us lessons about the need for resiliency, the need for collaboration across levels of government and with the private sector, and the fundamental role trust plays in achieving such collaboration. The United States does not have to wait to learn these lessons over again if an adversary inflicts a severe cyber crisis upon us. The nation must get ready now.

APPENDIXES

APPENDIX 1: ESTABLISHING A NATIONAL CYBER CRISIS CONTINGENCY IDENTIFICATION PROGRAM

The U.S. requires a program to guide effective, efficient identification of a National Cyber Crisis Contingencies (NCCCs) to help guide the establishment of the National Cyber Response Network (NCRN) and supporting capabilities. The nation should leverage learning from how to identify risks that guide planning for similar national risks including military conflicts, disaster preparedness including pandemics, hurricanes, fires and oil spills. The program must establish processes that result identify a set of National Cyber Crisis Contingencies (NCCCs) for planning purposes that illuminate for all stakeholders the national and economic security-level risks the U.S. faces and can be used to establish and assess the NCRN ability to manage and mitigate the risks.

Key priorities for establishing the NCCC identification program include:

- Analytical Rigor
 - ◇ Common understanding of national economic and security assets reliant on the digital environment
 - ◇ Common understanding of drivers of risks including threats and vulnerabilities
 - ◇ Ability to prioritize identified contingencies based on whole-of-nation risks and based on severe, but plausible, likelihood and impact
- Broad Stakeholder Input and Involvement
 - ◇ Both public and private sector organizations and leaders must guide the effort
 - ◇ Transparency of the process, data, and analysis used and conclusions
 - ◇ The NYCTF points to the process used to

establish the NIST Cyber Security Framework as a possible model

- Periodically publish key national cyber contingencies covering an appropriate range of:
 - ◇ Adversaries, their capabilities, and intent
 - ◇ Severity and duration of harms
 - ◇ Stakeholders necessarily involved in response and recovery

Key challenges for identifying prioritized NCCCs include:

- Requirement that NCCCs be established without prior experience, which is necessarily highly speculative
- Limitations on current ability to accurately characterize adversary capabilities
- A wide range of cyberattack possibilities
- Delineating potential harms due to limited knowledge of digital reliance at the organizational and national systemic level further complicated by fast-evolving technological and organizational change
- Willingness to articulate severe but plausible harms as the basis for planning

Recommended first steps in establishing a program:

- ONCD identify the Federal government organization to lead the NCCC identification effort¹⁴
- ONCD invite key public and private stakeholders, and establish planning process and objectives
- Identify a limited number of NCCCs for identification

- Prioritize full articulation of a single NCCC means to establish process and ensure stakeholder participation and satisfaction

The NYCTF believes this effort must have national-level priority, which could be achieved by establishing a senior-level steering committee involving both public and private leaders and firm timelines for tasks.

Recommended initial uses for NCCCs:

- Guide process of establishing NCRN including identification of key nodes in NCRN mapped to priority NCCCs
- Integrate with federal government planning process such as the NRP, NCIRP, Cyber Command, state, and municipal emergency response plans as well as contingencies and response planning addressed by the ARC and ISACs
- Leverage first set of NCCC to guide establishment of situational awareness capabilities and NCRN node criteria for capabilities assessment, exercises, and training

APPENDIX 2: MAP OF DRIVERS TO SCENARIOS

Global Politics

The Decline of Globalization—Decreases in International Collaboration and Enforcement of Norms

Since the 2008 global financial crisis, economic indicators have shown slower growth, rising inequality, and a decline in foreign direct investment. Many global multilateral trade talks and norm-building summits stalled, more trade agreements occurring as bilateral or regional agreements. Backlash stemming from anger about inequality and rising unemployment increased populist-nationalist sentiment in many countries. Governments around the world pushed increasingly protectionist policies. Notable examples include the U.K. decision to leave the European Union and the U.S. decision to withdraw from international agreements. Skepticism of international institutions increased as rising tensions between the U.S., China, and Russia led to a decrease in international collaboration, and building norms have become increasingly difficult. Great power competition splintered collaboration and norms around technology and the Internet around national lines.

Scenarios: 2, 3, 4

- Michael J. O’Sullivan, *The Levelling: What’s Next after Globalization*, First edition. (New York: PublicAffairs, 2019), 1–56.
- Patrick Diamond, ed., “Introductions,” in *The Crisis of Globalization: Democracy, Capitalism and Inequality in the Twenty-First Century* (I.B. Tauris, 2019), 1–24, <https://doi.org/10.5040/9781788316309>.
- Richard Fontaine, “Globalization Will Look Very Different After the Coronavirus Pandemic,” *Foreign Policy*, April 17, 2020, <https://foreignpolicy.com/2020/04/17/globalization-trade-war-after-coronavirus-pandemic/>.

- Sharma Ruchir, “Globalisation as We Know It Is Over—and Brexit Is the Biggest Sign Yet,” *the Guardian*, July 28, 2016, <https://www.theguardian.com/commentisfree/2016/jul/28/era-globalisation-brexit-eu-britain-economic-frustration>.

Great Power Competition with Russia/China

The U.S. is currently caught in global power competition with Russia and China over economic and security matters. Russia’s regional, political, and economic ambitions are at odds with American foreign policy and threatened by increasing NATO membership in Russia’s “near abroad.” Russia poses a national security threat to the U.S. as it has repeatedly engaged in military campaigns to place pressure on border NATO states and backs U.S. adversaries in Syria and the Middle East. China’s economic, military, and expansionist ambitions, such as the Belt and Road Initiative and military activity in the South China Sea, threaten U.S. regional and economic interests. The U.S. currently holds sanctions against Russia and is in a trade war with China. Friction between the U.S. and Russia/China extends into the cyber realm; both Russia and China have invested in cyber offensive capabilities.

Scenarios: 2, 4

- Anthony H. Cordesman and Grace Hwang, “The Broader Structure of U.S. Strategic Competition with China and Russia,” *The Biden Transition and U.S. Competition with China and Russia* (Center for Strategic and International Studies (CSIS), 2021), JSTOR, <https://www.csis.org/analysis/biden-transition-and-us-competition-china-and-russia-crisis-driven-need-change-us-strategy>.

- Lawrence Freedman, “Who Wants to Be A Great Power?,” *PRISM* 8, no. 4 (2020): 2–15, <https://www.jstor.org/stable/26918230>.
- Weixing Hu, “The United States, China, and the Indo-Pacific Strategy,” *China Review* 20, no. 3 (2020): 127–42, <https://muse.jhu.edu/article/764073>.
- Javier Solana, “Reconciling Great Power Competition with Multilateralism,” *Horizons: Journal of International Relations and Sustainable Development*, no. 7 (2016): 58–65, <https://www.cirsd.org/en/horizons/horizons-spring-2016--issue-no-7/reconciling-great-power-competition-with-multilateralism-?>
- Matthew Kroenig, “Introduction,” in *The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the U.S. and China*, 2020, 1–11.

Korean Peninsula Issues

For years, the potential for large-scale conflict in the Korean Peninsula had been a constant, but relatively low, risk. Recent acceleration of North Korea’s nuclear weapons development, increasingly confrontational rhetoric from Pyongyang, and concerns about potential regime instability have increased the risk of conflict. Major regional stakeholders include the U.S., Russia, China, Japan, and South Korea; however, global competition has reduced incentives for cooperation, and recent negotiations have been bilateral rather than multilateral summits. Negotiations in 2019 between the U.S. and North Korea failed; ongoing global competition has reduced pressure for North Korean denuclearization and cooperation incentives.

Scenario: 3

- Kiyoungh Chang and Choongkoo Lee, “North Korea and the East Asian Security Order: Competing Views on What South Korea Ought to Do,” *The Pacific Review* 31, no. 2 (March 4, 2018): 245–55, <https://doi.org/10.1080/09512748.2017.1397733>.
- Jong Kun Choi, “The Perils of Strategic Patience with North Korea,” *The Washington Quarterly* 38, no. 4 (October 2, 2015): 57–72, <https://doi.org/10.1080/0163660X.2015.1125829>.
- Nicholas D. Anderson, “Explaining North Korea’s Nuclear Ambitions: Power and Position on the

Korean Peninsula,” *Australian Journal of International Affairs* 71, no. 6 (November 2, 2017): 621–41, <https://doi.org/10.1080/10357718.2017.1317328>.

- Michael J. Mazarr et al., *The Korean Peninsula: Three Dangerous Scenarios* (RAND Corporation, 2018), <https://doi.org/10.7249/PE262>.

Friction with Iran and in the Middle East

Recent activities of American foreign policy, such as the withdrawal from the Joint Comprehensive Plan of Action (JCPOA) in 2018, recognition of Israeli sovereignty in disputed Syrian and Palestinian land, and unilateral measures exacerbated regional tensions in the Middle East. The continued U.S. presence in Iraq, an imposed conventional weapons embargo, and economic sanctions against Iran further contributed to the tension between the two countries, inciting military frictions with Iran and Iran-backed militias. Iran has repeatedly threatened to cancel its nuclear agreements and withdraw from the nuclear Non-Proliferation Treaty. Rising tensions and future involvement by Russia, China, and Europe in Iran could further destabilize the region.

Scenario: 1

- Sima Shine and Eldad Shavit, “Iran and the United States: Breaking the Rules of the Game?” (Institute for National Security Studies, 2020), <https://www.jstor.org/stable/resrep25531>.
- Michael Singh, “Iran and America,” *Horizons: Journal of International Relations and Sustainable Development*, no. 16 (2020): 144–59, <https://www.jstor.org/stable/48573756>.
- Rex Brynen, “Exploring US Engagement in the Middle East: A Crisis Simulation” (Atlantic Council, 2016), JSTOR, <https://www.jstor.org/stable/resrep03470>.
- Ross Harrison, “U.S. Interests Revisited,” U.S. Foreign Policy Towards the Middle East (Arab Center for Research & Policy Studies, 2019), JSTOR, <https://www.jstor.org/stable/pdf/resrep19950.5.pdf>.
- Jin Liangxiang, “China and Middle East Security Issues: Challenges, Perceptions and Positions.” (Istituto Affari Internazionali (IAI), 2020), JSTOR, <https://www.jstor.org/stable/resrep26107>.

Taiwan Crisis/South Sea Crisis

China has ongoing sovereignty disputes in the South China Sea. The government maintains a “one China” policy in the region. In the South China Sea, China uses assertive military activity to ignore neighboring country claims over zones and islands, and to disregard UN conventions on maritime law. Taiwan (officially the Republic of China) is located off the southern coast of China and, while economically bound, possesses an independent democratically elected government. Since 1992, China and Taiwan have had a tacit agreement that Taiwan will not seek independence. In 2019, government leaders in Taiwan rejected the consensus in a national speech stating that the “one China, two systems” framework was no longer acceptable. China has since increased military activity in the region, deploying missiles and conducting military drills along the Taiwan Strait. To protect its regional interests and maintain alliances, the U.S. has challenged China’s territorial claims by conducting Freedom of Navigation Operations (FONOPS) and providing support to allies in Southeast Asia. Crisis in the region could compel the U.S. to provide aid to honor existing treaties, potentially leading to conflict with mainland China.

Scenario: 2

- Ping-Kuei Chen, Scott L. Kastner, and William L. Reed, “A Farewell to Arms?: US Security Relations with Taiwan and the Prospects for Stability in the Taiwan Strait,” in *Taiwan and China*, ed. Lowell Dittmer, 1st ed., Fitful Embrace (University of California Press, 2017), 221–38, <http://www.jstor.org/stable/10.1525/j.ctt1w76wpm.15>.
- Julie Yang et al., “‘Digital Nation, Smart Island’: Building a Workforce for the Digital Economy,” Perspectives on Taiwan (Center for Strategic and International Studies (CSIS), 2019), JSTOR, <https://www.jstor.org/stable/resrep22549.6>.
- Alice D. Ba, “Staking Claims and Making Waves in the South China Sea: How Troubled Are the Waters?,” *Contemporary Southeast Asia* 33, no. 3 (2011): 269–91.
- Peter Van Ham, Francesco Saverio Montesano, and Frans Paul van der Putten, “The Scenario,” in *A South China Sea Conflict: Implications for European Security* (Clingendael Institute, 2016), 13–22,

<http://www.jstor.org/stable/resrep05541.6>.

- Natasha Kassam and Richard McGregor, “Taiwan’s 2020 Elections” (Lowy Institute for International Policy, 2020), JSTOR, <https://www.jstor.org/stable/resrep25092>.

Rise of Cybercrime and Illicit Enabled Activity

Cybercrime is an ongoing and persistent threat that continues to increase each year. The anonymity afforded by the Internet has made cybercrime a low-risk, high-reward venture for both state and non-state actors. Current predictions estimate that cybercrime could cost \$6 trillion in damages globally in 2021, with costs expected to increase as cybercrime continues to rise. The U.S. and global law enforcement struggle to gain an advantage over cybercriminals and attackers. While a majority of cybercrime activity is transnational, advancement in international cooperation to define rules and norms of behavior has stalled as great power competition has blocked consensus. Increased use of cyber by nation-states and proxy actors has diminished shared incentives.

Scenario: 3

- Chris Bronk, “Cybercrime and Punishment,” in *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security* (Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC, 2016), 138–49.
- Allison Peters and Amy Jordan, “Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime,” (Third Way, 2019), JSTOR, <https://www.jstor.org/stable/resrep20150>.
- Michael Garcia and Anisha Hindocha, “Where Are We Now?: Examining the Trump Administration’s Efforts to Combat Cybercrime,” (Third Way, 2020), JSTOR, <https://www.jstor.org/stable/resrep25042>.
- Nicholas Davis and Klaus Schwab, “Cyber Risks,” in *Shaping the Future of the Fourth Industrial Revolution*, vol. 72 (Currency, 2018), 114–20.
- John P. Carlin and Garrett M. Graff, “Introduction: The Code War,” in *Dawn of the Code War: America’s Battle against Russia, China, and the Rising Global Cyber Threat*, First edition (New York: PublicAffairs, 2018), 31–64.

Breakdown of Social Norms

The 2013 and 2015 UN GGE had some success in promoting nonbinding cyber norms and confidence-building measures that were endorsed by the global community. International collaboration and discussion to identify and promote further norms of behavior fragmented at the 2017 UN GGE as competition and ideological differences blocked consensus. Work to identify and operationalize cyber norms is now fragmented into multiple groups in the UN (GGE and OWEG), expert commissions (The Global Commission on the Stability of Cyberspace), industry coalitions (the Tech Accord), and multistakeholder collectives (The Paris Call for Trust and Security in Cyber Space).

Scenario: 4

- James Andrew Lewis, “Revitalizing Progress in International Negotiations on Cyber Security,” in *Getting beyond Norms: New Approaches to International Cyber Security Challenges*, ed. Fen Osler Hampson and Michael Sulmeyer (Centre for International Governance Innovation, 2017), 13–18, <https://www.jstor.org/stable/resrep05241.6>.
- Laurie Laybourn-Langton and Lesley Rankin, *Our Responsibility: A New Model of International Cooperation for the Era of Environmental Breakdown* (Institute for Public Policy Research (IPPR), 2019), <https://www.jstor.org/stable/resrep21891.9>.
- Christian Ruhl et al., “Front Matter,” *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (Carnegie Endowment for International Peace, 2020), JSTOR, <https://www.jstor.org/stable/resrep24286.1>.

The Digital Divide Continues to Grow within Nations and across the Globe

While many have touted the ability for technology and Internet access to help developing countries and lower-income communities access education and become integrated into the global economy, the stark reality shows that more often these communities are left behind. The majority of wealth in the digital economy is held by the U.S and China, while developing countries in Africa and Latin America are further behind. Internet penetration trends demonstrate that Internet density, or

users by population, is higher within industrial countries and affluent communities. Estimates of 2020 of Internet penetration show that Internet density increased in developed countries to over 50 percent of the population, but penetration levels in developing nations remain below 10 percent of the global population. Without interventions to bridge digital access, the skewed distribution of wealth in the digital economy and Internet penetration will widen the digital divide and intensify inequality and existing socioeconomic disparities.

Scenario: 4

- Simona R. Soare, “Digital Divide?: Transatlantic Defence Cooperation on Artificial Intelligence” (European Union Institute for Security Studies (EUISS), 2020), JSTOR, <https://www.jstor.org/stable/resrep25027>.
- Christian Fuchs and David Chandler, “Introduction,” in *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data* (University of Westminster Press, 2019), 1–20, <http://www.jstor.org/stable/j.ctvckq9qb.3>.
- Ishaq Ashfaq, “On the Global Digital Divide,” *Finance and Development*, International Monetary Fund, September 2001, <https://www.imf.org/external/pubs/ft/fandd/2001/09/ishaq.htm>.
- “‘Digital Divide’ Will Worsen Inequalities, without Better Global Cooperation,” *UN News*, September 4, 2019, <https://news.un.org/en/story/2019/09/1045572>.

Shifting Global Balance of Power away from the U.S. and toward China

The rise of China as a leading world economy has shifted power away from the U.S., as China increases its sphere of influence. As the second-largest world economy, China has promoted massive infrastructure projects in Asia and Europe through its Belt and Road Initiative, and infrastructure and development projects to support countries in Africa and Latin America. China’s ambitious economic plans and military assertiveness threatens U.S. economic and national security interests as China acquires more influence among countries and in international policy discussions.

Scenario: 2

- John G. Ikenberry, “Between the Eagle and the Dragon: America, China, and Middle State Strategies in East Asia,” *Political Science Quarterly* 131, no. 1 (March 2016): 9–43, <https://doi.org/10.1002/polq.12430>.
- Nick Bisley et al., “To Choose or Not to Choose: How to Deal with China’s Growing Power and Influence” (Australian Strategic Policy Institute, 2014), JSTOR, <http://www.jstor.org/stable/resrep04059>.
- Graham T. Allison, “Where Do We Go From Here,” in *Destined for War: Can America and China Escape Thucydides’s Trap?*, 2017, 214–31.
- Weixing Hu, “The United States, China, and the Indo-Pacific Strategy: The Rise and Return of Strategic Competition,” *China Review* 20, no. 3 (2020): 127–42, <https://www.jstor.org/stable/26928114>.
- Joshua R. Itzkowitz Shiffrin and Michael Beckley, “Debating China’s Rise and U.S. Decline,” *International Security* 37, no. 3 (2012): 172–81.
- Douglas H. Paal, “How Washington and Regional Partners Can Manage China’s Rise,” *America’s Future in a Dynamic Asia* (Carnegie Endowment for International Peace, 2019), JSTOR, <https://www.jstor.org/stable/resrep20999.8>.

U.S. Domestic Politics

Growing Political Divides

Partisan divides have grown within the United States dividing politicians and communities. Polarization continues to intensify degrading trust in community members with different perspectives, as voters believe differences are increasingly about core American values rather than policy differences. Societal tensions exacerbate the growing division threatening U.S. democracy.

Scenario: 4

- Darrell M. West, *Divided Politics, Divided Nation: Hyperconflict in the Trump Era*, Washington, D.C.: Brookings Institution Press, 2019.

Impact on Social Norms and Trust in Government

Since the recession in 2008, public trust levels in government and institutions have been low. Trust levels and public sentiment about the government and institutions have remained relatively stable. Both positive or negative changes in sentiment are reliant on perceptions about government efficiency in managing the coronavirus spread, availability of a vaccine, and the financial resources to alleviate financial strain.

Scenario: 4

- Jill Suttie, “How Does COVID-19 Affect Trust in Government?,” *Greater Good Magazine*, July 21, 2020, https://greatergood.berkeley.edu/article/item/how_does_covid_19_affect_trust_in_government.

Economic

The Decline of Globalization—Nationalistic Economic Policies

Since the 2008 global financial crisis, economic indicators have shown slower growth, rising inequality, and a decline in foreign direct investment. Many governments enacted more protectionist policies to deal with domestic concerns over inequality and job scarcity. Notable examples include Brexit and the America First foreign policy promoted under the Trump Administration, as well as the U.S.-China trade war. Recent policies by the U.S. and other governments have placed increased restrictions over the import and export of critical technologies. In response to COVID-19, many countries further restricted foreign investments and exports on redefined critical national assets, such as PPE.

Scenarios: 1, 2, 3, 4

- Michael J. (Michael Joseph) O’Sullivan, *The Levelling: What’s next after Globalization*, First edition. (New York: PublicAffairs, 2019).
- Patrick Diamond, ed., “Introduction,” in *The Crisis of Globalization: Democracy, Capitalism and Inequality in the Twenty-First Century* (I.B. Tauris, 2019), 1–24.
- Richard Fontaine, “Globalization Will Look Very Different After the Coronavirus Pandemic,” *Foreign Policy* (blog), April 17, 2020, <https://foreignpolicy>.

com/2020/04/17/globalization-trade-war-after-coronavirus-pandemic/.

- Ruchir Sharma, “Globalisation as We Know It Is Over—and Brexit Is the Biggest Sign Yet,” the Guardian, July 28, 2016, <https://www.theguardian.com/commentisfree/2016/jul/28/era-globalisation-brexit-eu-britain-economic-frustration>.

Global Recession

To combat the COVID-19 pandemic, governments were forced to close borders and enact global economic shutdown measures, which led to a devastating economic recession. The World Bank forecasted a global economic contraction by 5.2 percent, making it the deepest recession since the Second World War. Stress on the global supply chain from border closures and factory shutdowns led to global shortages from halted global manufacturing and shipping.

Scenario: 1

- Jonathan Eaton et al., “Trade and the Global Recession,” *The American Economic Review* 106, no. 11 (2016): 3401–38.
- William Reinsch and Jack Caporal, “International Economic Projections,” Key Trends in the Global Economy through 2030 (Center for Strategic and International Studies (CSIS), 2020), 5–17, JSTOR, <https://www.jstor.org/stable/resrep26050.5>.
- Daniel F. Runde and Sundar R. Ramanujam, “Recovery with Resilience” (Center for Strategic and International Studies (CSIS), 2020), JSTOR, <https://www.jstor.org/stable/resrep26011>.

Decoupling and Trade War with China

Since 2018, when the U.S imposed increased trade tariffs on China, the two countries have been engaged in an ongoing trade war. U.S concerns over China’s economic espionage and investment in foreign communications networks fueled policy decision to impose tariffs and impose export restrictions. Recent U.S. restrictions targeted Chinese technology companies, like Huawei, to safeguard U.S. digital assets from China. China has a large share in the global supply chain of technology, and competition over advanced technologies has encouraged

the U.S. to consider decoupling to protect its national interests, despite potential economic sacrifices. The stress COVID-19 placed on the global supply chain has increased global concerns about overreliance on China and could accelerate decoupling between the U.S. and China economies.

Scenario: 2

- Matthew P. Goodman, Dylan Gerstel, and Pearl Risberg, “Beyond the Brink: Escalation and Conflict in U.S.-China Economic Relations” (Center for Strategic and International Studies (CSIS), 2019), <https://www.jstor.org/stable/resrep22381>.
- Refk Selmi, Youssef Errami, and Mark E. Wohar, “What Trump’s China Tariffs Have Cost U.S. Companies?,” *Journal of Economic Integration* 35, no. 2 (2020): 282–95, <https://www.jstor.org/stable/26917205>.
- Marc Lanteigne, “The Spiralling Effects of the Sino-American Trade War” (Norwegian Institute of International Affairs (NUPI), 2020), JSTOR, <https://www.jstor.org/stable/resrep25746>.
- Robert A. Manning, “Who Dominates the Future?,” The China Challenge to an Inclusive Asia-Pacific Regional Trade Architecture (Atlantic Council, 2018), 7–8, JSTOR, <https://www.jstor.org/stable/resrep20934.6>.
- Roland Rajah, “East Asia’s Decoupling” (Lowy Institute for International Policy, 2019), JSTOR, <https://www.jstor.org/stable/resrep25089>.
- Darren J. Lim and Victor Ferguson, “Conscious Decoupling,” in *China Dreams*, ed. Jane Golley et al. (ANU Press, 2020), 118–32, DOI: 10.22459/CSY.2020.
- “The Pivot and China,” What Asia Wants from the US (Asan Institute for Policy Studies, 2018), 55–60, JSTOR, <https://www.jstor.org/stable/resrep20691.12>.

Technology

Artificial Intelligence/Machine Learning

Advances in artificial intelligence and machine learning

will have enormous economic, societal, and geopolitical impacts. Artificial intelligence components are increasingly embedded in many aspects of life and business, introducing new technological challenges and risks. Potential risks include existing cybersecurity threats and vulnerabilities accessing cloud computing systems; concerns over data privacy and data management; transparency in the usages of decision making; and algorithmic bias. Additional challenges stem from geopolitics and different perspectives on data protection, privacy, autonomy, transparency, and accountability.

Scenarios: 1, 3, 4

- Camino Kavanagh, “Artificial Intelligence,” *New Tech, New Threats, and New Governance Challenges* (Carnegie Endowment for International Peace, 2019), 13–23, JSTOR, <https://www.jstor.org/stable/resrep20978.5>.
- Brian Katz, “The Intelligence Edge” (Center for Strategic and International Studies (CSIS), 2020), JSTOR, <https://www.jstor.org/stable/resrep24247>.
- Francisco L. Loaiza et al., “Utility of Artificial Intelligence and Machine Learning in Cybersecurity” (Institute for Defense Analyses, 2019), JSTOR, <https://www.jstor.org/stable/resrep22692>.
- Paul Scharre, Michael C. Horowitz, and Robert O. Work, “AI Safety Concerns and Vulnerabilities,” *Artificial Intelligence* (Center for a New American Security, 2018), 11–16, JSTOR, <https://www.jstor.org/stable/resrep20447.7>.

5G Networks

5G technology will massively improve data speeds and the capability for high-capacity and ultra-low latency communications, making it a critical component for future applications that require highly reliable and near-instantaneous access to massive amounts of data. 5G will enable advancements, like smart cities or driverless cars, to become possible on a commercial scale. The transformative nature of 5G has made it heavily politicized in U.S.-China global power competition.

Scenario: 2

- Eurasia Group, “Eurasia Group White Paper: The Geopolitics of 5G” (Eurasia Group, November

15, 2018), [https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public\(1\).pdf](https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf).

- Elsa B. Kania, “The Promise of 5G,” *Securing Our 5G Future* (Center for a New American Security, 2019), JSTOR, <https://www.jstor.org/stable/resrep20451.4>.
- Rajiv Shah, “5G and Cybersecurity,” *Ensuring a Trusted 5G Ecosystem of Vendors and Technology* (Australian Strategic Policy Institute, 2020), JSTOR, www.jstor.org/stable/resrep26116.9.
- Benjamin Fricke, “Artificial Intelligence, 5G and the Future Balance of Power” (Konrad Adenauer Stiftung, 2020), JSTOR, <https://www.jstor.org/stable/resrep25281>.
- “America Does Not Want China to Dominate 5G Mobile Networks,” *The Economist*, April 11, 2020, <https://www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks>.

IoT and Embedded Devices

The Internet of Things (IoT) comprises physical devices that can connect to the Internet, collect, and share data. IoT is a central component of the expanding interconnectedness between the digital and physical world. While IoT can provide many societal benefits, many IoT devices are not designed with security in mind. Unsecured IoT devices can be targeted in cyberattacks to create botnets or gain access to connected networks. Current estimates of IoT devices range from 25 to 30 billion, and usage is expected to increase. Despite concerns over the cyber and physical security risks posed by IoT devices, there are no global standards for IoT and related devices.

Scenarios: 1, 2

- Nicole A. Drepa, “Sustainable Cities and the Internet of Things (IOT) Technology,” *Consilience*, no. 22 (2020): 39–47, <https://doi.org/10.7916/consilience.vi22.6742>.
- James Andrew Lewis, “Managing Risk for the Internet of Things,” *Managing Risk for the Internet of Things* (Center for Strategic and International Studies (CSIS), 2016), JSTOR, <https://www.jstor.org/stable/resrep23321.4>.

- Jason Hong, “What Makes Security for IoT Different?,” *Toward a Safe and Secure Internet of Things* (New America, 2016), 5–8, JSTOR, <https://www.jstor.org/stable/resrep10509.5>.
- Atul Mahamuni, “Internet of Things, Machine Learning, and Artificial Intelligence in the Modern Supply Chain and Transportation,” *Defense Transportation Journal* 74, no. 1 (2018): 14–17, www.jstor.org/stable/26430583.
- Michel Girard, “Standards for Cybersecure IoT Devices,” (Centre for International Governance Innovation, 2020), JSTOR, www.jstor.org/stable/resrep25237.
- Nayan B. Ruparelia, “Transitioning to the Cloud,” in *Cloud Computing* (The MIT Press, 2016), 195–218, [10.7551/mitpress/9780262529099.001.0001](https://doi.org/10.7551/mitpress/9780262529099.001.0001).

Remote Work

Advances in networks, cloud computing, and AI technology enable more businesses and workers to work remotely using new tools and applications for collaboration and to access shared content. Since society adapted to mass quarantine measures during the coronavirus pandemic, more people are working from home. There are now over 300 million customers registered for services like Microsoft Teams, Zoom, Google Meet, and Cisco Webex.

Scenarios: 1,4

- Matthew Dey et al., “Ability to Work from Home,” *Monthly Labor Review*, 2020, 1–19, <https://www.bls.gov/opub/mlr/2020/article/ability-to-work-from-home.htm>.
- “Is the Office Finished?,” *The Economist*, September 10, 2020, <https://www.economist.com/leaders/2020/09/12/is-the-office-finished>.
- Matt Clancy, “Remote Work Is Here to Stay,” *The Economist Intelligence Unit*, May 27, 2020, <https://eiuperspectives.economist.com/technology-innovation/remote-work-here-stay>.

Cloud Technology

Cloud technology is projected to see sharply increased usage from governments, the private sector, and individual consumers in the coming decade. This shift places an extraordinary amount of trust and responsibility onto the concentrated market of cloud service providers (CSPs). As the security of the cloud covers a multitude of services, technologies, and markets, it therefore has a wide breadth of potential vulnerabilities and threats. While there is some evidence that a shift to cloud computing would mitigate some present cybersecurity threats, there are still unquantifiable and likely growing risks resulting from increased dependence on the cloud; these include risks to data privacy and integrity, the functionality of critical infrastructure and systems reliant on cloud technology, and the systemic resilience of CSPs themselves.

Scenarios: 2, 3, 4

- Tim Maurer and Garrett Hinck, “Cloud Security,” *CloudSecurity*(CarnegieEndowmentforInternationalPeace, 2020), 22–37, JSTOR, www.jstor.org/stable/resrep25787.2.
- Frank Cilluffo, Ron Ritchey, and Timothy Tinker, “Cloud Computing Risks and National Security Keeping Pace With Expanding Technology” (Center for Cyber and Homeland Security at Auburn University, 2010), JSTOR, <https://www.jstor.org/stable/resrep21462>.
- “Resiliency in the Cloud,” *IBM Global Technology Services*, June 2015, <https://www.ibm.com/downloads/cas/AVY5QYG0>.

Social Technologies (VR/Deep Fakes)

AI-generated media, such as Deep fakes and Virtual Reality, possess the potential to manipulate reality and spread misinformation and disinformation. Deep fakes, or AI-generated images or videos, have been used to spread fake news, conspiracy theories, and commit financial fraud. Deep fake technology can be incredibly sophisticated and generate realistic images that are difficult to detect as fake. Virtual Reality (VR) technology is only just reaching the point where companies are mass marketing VR technology to consumers. VR enables users to interact in seemingly real or physical ways with an audiovisual computer-generated simulation. While not yet realized, there are concerns that VR could be used in military applications to manipulate perceptions of reality.

Scenario: 4

- Hannah Smith and Katherine Mansted, “Weaponised Deep Fakes,” *Weaponised Deep Fakes* (Australian Strategic Policy Institute, 2020), 11–14, JSTOR, www.jstor.org/stable/resrep25129.7.
- Jon Bateman, “Policy Implications,” *Deepfakes and Synthetic Media in the Financial System* (Carnegie Endowment for International Peace, 2020), 26–32, JSTOR, www.jstor.org/stable/resrep25783.14.
- Rick Meessen, Bianca Torossian, and Frank Bekkers, “Emerging Technologies and Capabilities in Hybrid Threats,” *A Horizon Scan of Trends and Developments in Hybrid Conflicts Set to Shape 2020 and Beyond* (Hague Centre for Strategic Studies, 2020), 27–40, JSTOR, www.jstor.org/stable/resrep24197.6.

Facial Recognition

Facial recognition technology utilizes images or videos to create detailed biometric maps of individuals that can be used for identification or to conduct sentiment analysis. While facial recognition systems are spreading around the world, there is growing citizen backlash against the usage of facial recognition by companies and government, particularly law enforcement. The technology is extremely intrusive and there are privacy, consent, and transparency concerns around the usage of the technology and concerns over the management of the biometric data. Facial recognition has raised issues of government and law enforcement surveillance.

Scenario: 3

- Charles J. Dunlap and Charlie J. Dunlap, “The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict,” *Georgetown Journal of International Affairs*, 2014, 108–18.
- Steven Feldstein, “Types of AI Surveillance,” *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace, 2019), 16–21, JSTOR, <https://www.jstor.org/stable/resrep20995.8>.
- Edward Santow, “Can Artificial Intelligence Be Trusted with Our Human Rights?,” *AQ: Australian Quarterly* 91, no. 4 (2020): 10–17, <https://www.jstor.org/stable/26931483>.
- “As Face-Recognition Technology Spreads, so Do

Ideas for Subverting It,” *The Economist*, August 17, 2019, <https://www.economist.com/science-and-technology/2019/08/15/as-face-recognition-technology-spreads-so-do-ideas-for-subverting-it>.

Cyber Ecosystem Instability

Offense Dominance in Cyber Leading to Instability

In 2018, the U.S. issued a new cyber policy authorizing the use of offensive cyber operations to deter adversaries by imposing costs on their operations. Proponents of the policy suggest that the policies could have a stabilizing effect as repeated adversary engagement would lead to a tacit agreement of acceptable behavior in cyber. Critics of the policy are cautious that such a policy could lead to a risk of inadvertent escalation between adversaries.

Scenario: 3

- Michael P. Fischerkeller and Richard J. Harknett, “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation,” *The Cyber Defense Review*, 2019, 267–87, <https://www.jstor.org/stable/26846132>.
- Benjamin Jensen and Brandon Valeriano, “What Do We Know about Cyber Escalation?” (Atlantic Council, 2019), JSTOR, <https://www.jstor.org/stable/resrep20705>.
- Erica D. Borghard and Shawn W. Lonergan, “Cyber Operations as Imperfect Tools of Escalation,” *Strategic Studies Quarterly* 13, no. 3 (2019): 122–45.
- Peter Leach, “Nuclear Stability–Cyber Instability: A New Look at an Old Cold War Theory,” *Small Wars Journal*, August 29, 2018, <https://smallwarsjournal.com/jrnl/art/nuclear-stability-cyber-instability-new-look-old-cold-war-theory>.

Nation-State Adversary Preemptively Attacks U.S. Critical Infrastructure to Disrupt Response to an Attack Elsewhere

Critical infrastructure are assets deemed as fundamental to the functioning of society and the economy. Due to interdependence with the Internet, critical infrastructure has become increasingly fragile. A disruptive or destruc-

tive cyberattack on a critical infrastructure sector can have immediate and direct impacts on the day-to-day life and safety of people. An attack on one sector could also lead to cascading effects on other sectors, adding severity to the potential consequences. Cyberattacks targeting critical infrastructure are not unprecedented. In 2007 Estonia faced a series of cyberattacks that impacted financial online banking and government emails, and in 2015 Ukraine was hit by a cyberattack that disabled a portion of Ukraine's electrical grid.

Scenario: 1

- Ryan J. Hayward, "Evaluating the 'Imminence' of a Cyber Attack for Purposes of Anticipatory Self-Defense," *Columbia Law Review* 117, no. 2 (2017): 399–434.
- Sanjay Goel, "National Cyber Security Strategy and the Emergence of Strong Digital Borders," *Connections* 19, no. 1 (2020): 73–86, <https://www.jstor.org/stable/26934537>.
- Tyson Macaulay and Centre for International Governance, "The Danger of Critical Infrastructure Interdependency," *Governing Cyberspace during a Crisis in Trust* (Centre for International Governance Innovation, 2019), JSTOR, www.jstor.org/stable/resrep26129.16.

A Higher Level of Dependence on Networks in the U.S.

Advances in network connectivity have paved the way for new data and network-dependent technologies—such as IoT, blockchain, and cloud computing—to reconstruct enterprise architecture across sectors. Digital transformation has made reliance on shared data and networks central to the digital economy. Increased reliance on technology introduces vulnerabilities and risks to businesses and society through interconnected networks, software vulnerabilities, IoT, and cyber-physical systems.

Scenarios: 1, 4

- William Lehr et al., "Whither the Public Internet?," *Journal of Information Policy* 9 (2019): 1–42, <https://www.jstor.org/stable/10.5325/jinfopoli.9.2019.0001>.
- Prabhudev Konana, "The Economy Is Too Dependent

on the Internet," *Psychology Today*, November 27, 2017, <https://www.psychologytoday.com/us/blog/the-fundamentals/201711/the-economy-is-too-dependent-the-internet>.

Dependence of the U.S. on Global Supply Chain

For years, U.S. corporations have moved manufacturing offshore, making the U.S. reliant on the global supply chain. Depending on the global supply chain increases risks from reduced transparency of third-party supply chains. China is the world's leading exporter and manufacturer of goods and a supply chain hub, particularly for technology. The U.S. is reliant on the Chinese supply chains for strategic sectors in pharmaceuticals and information communication technology. Economic and security tensions between the two countries further increase supply chain risk to U.S. national interests and corporations.

Scenario: 1

- Runde and Ramanujam, "Recovery with Resilience" (Center for Strategic and International Studies (CSIS), 2020), JSTOR, www.jstor.org/stable/resrep26011.
- Aaron Friedberg, "The United States Needs to Reshape Global Supply Chains," *Foreign Policy*, May 8, 2020, <https://foreignpolicy.com/2020/05/08/united-states-reshape-global-supply-chains-china-reglobalization/>.
- Yoganathan, "Building Resilient Supply Chains," *Building Critical Supply Chain Resilience in the Wake of COVID-19* (S. Rajaratnam School of International Studies, 2020), 8–12, JSTOR, www.jstor.org/stable/resrep25424.6.
- Donald Lessard, "Uncertainty and Risk in Global Supply Chains," in *Global Value Chains in a Changing World*, ed. Deborah Elms and Low, Patrick (WTO Publications, 2013), 195–221, https://www.wto.org/english/res_e/booksp_e/aid4tradeglobalvalue13_e.pdf.

Adversary Targets Critical Allies' Relationships Leading the U.S. into Undermining Actions

For years, the U.S. established international alliances to achieve U.S. national security and global influence. The

U.S. maintains close ties with allies and partners to develop policies, strategies, and operations against potential adversaries and to assure allies of U.S. credibility to protect allies from adversaries. Russia and China both engage in activities to undermine U.S. alliances and credibility. Cyberattacks, disinformation campaigns, and economic coercion fall below the military threshold and can complicate existing treaties to aid allies against adversaries.

Scenario: 2

- Anthony H. Cordesman, Arleigh A. Burke, and Max Molot, “U.S. Military Forces Affecting (and Affected By) China, the Pacific, the South China Sea, and Indian Ocean,” *China and the U.S.* (Center for Strategic and International Studies (CSIS), 2019), 256–67, JSTOR, www.jstor.org/stable/resrep22586.25.
- Elizabeth Rosenberg, Peter E. Harrell, and Ashley Feng, “Policy Recommendations,” *A New Arsenal for Competition* (Center for a New American Security, 2020), 39–48, JSTOR, www.jstor.org/stable/resrep24222.8.
- John Hemmings, “Pacific Trident III,” (Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020), JSTOR, <https://www.jstor.org/stable/resrep25712>.

Systemic Attack Advantages

Critical Services Going Remote Will Make Attack Surfaces Multiply Exponentially

COVID-19 accelerated enterprise digital transformation across all industries and sectors, as quarantine measures prompted the transition to remote work and offering customer services online. Even sectors, like government, healthcare, and banking, had prior restrictions on digital work and services relaxed. The transition increases cybersecurity risks as workers and customers access content through unsecured networks and devices. The expanded usages of application services also introduce new vulnerabilities from application software and third parties, increasing organization attack surfaces.

Scenario: 1

- Venky Anant et al., “A Dual Cybersecurity Mindset for the Next Normal,” *McKinsey & Company*, July 7, 2020, <https://www.mckinsey.com/business->

[functions/risk/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal](https://www.mckinsey.com/business-functions/risk/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal).

- Patrick Spencer, “Cyberattacks on Applications Grow Exponentially, Pose Serious Risk,” *Security Boulevard*, July 29, 2020, <https://securityboulevard.com/2020/07/cyberattacks-on-applications-grow-exponentially-pose-serious-risk/>.

Widespread Availability and Rapid Adoption of Nation-State Attack Tools

The commodification and proliferation of cyber offensive tools have lowered the barrier to entry for non-state and nation-state actors to use cyber tools for domestic surveillance, economic gain, and geopolitical impact. More nation-states can now use tools and capabilities to carry out attacks at a level of sophistication previously held by a few states. The increasing availability of marketplaces and information exchanges to share and sell cyber tools will increase the prevalence of cyberattacks, making it more difficult for defenders to match the pace of attackers.

Scenario: 3

- Ryan J. Hayward, “Evaluating the ‘Imminence’ of a Cyber Attack for Purposes of Anticipatory Self-Defense,” *Columbia Law Review*, vol. 117, no. 2, 2017, pp. 399–434. JSTOR, www.jstor.org/stable/44159464.
- Lesley Seebeck, *Not the Cyberterrorism You Thought*, edited by Isaac Kfir and John Coyne, Australian Strategic Policy Institute, 2020, pp. 75–80, *Counterterrorism Yearbook 2020*, www.jstor.org/stable/resrep25133.17.

Ability to Hide on the “Dark Web”

The Dark Web is a collection of thousands of websites that use anonymity tools to encrypt web traffic in layers, hiding the IP addresses of users and web servers. The anonymity provided by the Dark Web protects users from surveillance and censorship and is also used by malicious actors. Criminal activity on the Dark Web includes marketplaces that sell illegal goods and services, including marketplaces and information exchanges for cyber-attack tools.

Scenario: 3

- Michael Chertoff, Toby Simon, and Global Commission on Internet Governance, “The Impact of the Dark Web on Internet Governance and Cyber Security,” *Cyber Security in a Volatile World* (Centre for International Governance Innovation, 2017), 29–36, JSTOR, <http://www.jstor.org/stable/resrep05239.7>.
- Roshni Chakraborty, “The Deep Web,” *Harvard International Review* 39, no. 4 (2018): 18–21, <https://www.jstor.org/stable/26617373>.
- DC Derrick et al., “Cyber-Sophistication Assessment Methodology for Public-Facing Terrorist Web Sites,” *Journal of Information Warfare* 16, no. 1 (2017): 13–30.
- Calum Jeffray and Tobias Feakin, “Underground Web” (Australian Strategic Policy Institute, 2015), JSTOR, <http://www.jstor.org/stable/resrep04074>.

Widespread/Ease of Accessibility of Social Media

Social media now penetrates more than 50 percent of the world’s population and is widely used across society for communication and information consumption. Non-state and nation-state actors exploit the technology behind social media and user trust in media platforms to steal mission-critical information, commit identity theft, and spread mis- and disinformation. Vulnerabilities within social media platforms and third-party apps are also leveraged in cyberattacks to gain access to computer devices and information.

Scenario: 4

- Scott E. Solomon, “Threats and Vulnerabilities—What Is Different from the Past?,” *Social Media* (Air University Press, 2017), 3–8, JSTOR, <http://www.jstor.org/stable/resrep13937.7>.

Systemic Defensive Weaknesses

Attribution Errors in the Case of Simultaneous but Unrelated Attacks

Cyber threat actors employ a variety of tools and methods to evade detection and obfuscate their activity. Sophisticated nation-state actors can use layers of compromised

third-party networks for their cyberattacks to misdirect attribution. Deception techniques and false flag campaigns further add to the complexity of attribution.

Scenario: 3

- Jon Bateman, “Understanding the Problem,” *War, Terrorism, and Catastrophe in Cyber Insurance* (Carnegie Endowment for International Peace, 2020), 10–26, JSTOR, https://carnegieendowment.org/files/Bateman_-_Cyber_Insurance_-_Final.pdf.
- Amanda G. Hill, “Analysis,” *The Ultimate Challenge* (Air University Press, 2019), 13–24, JSTOR, <https://www.jstor.org/stable/resrep24884.2>.
- Sanjay Goel, “How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race,” *Connections* 19, no. 1 (2020): 87–95, <https://www.jstor.org/stable/26934538>.

Overconfidence in Attribution Methods

Advances in digital forensics tools and recent successful cases of attribution have propelled the notion that technological advances will help improve attribution. The analysis of state and non-state adversaries and activity for attribution is a complicated process because of misdirection, use of proxy actors, and changes in adversary tools and techniques. Attribution is influenced not only by available evidence but also by geopolitical factors and the credibility of investigators.

Scenario: 3

- Matthew Crosston, “Virtual Patriots and a New American Cyber Strategy,” *Strategic Studies Quarterly* 6, no. 4 (2012): 100–118.
- Gregory Conti and Robert Fanelli, “How Could They Not,” *The Cyber Defense Review* 4, no. 2 (2019): 49–64, www.jstor.org/stable/26843892.

Lack of International Resolution Methods

Since the failure of the 2017 GGE, international cooperation to advance cyber norms has splintered into UN groups (GGE and OWEG), expert commissions, industry coalitions, and multistakeholder collectives that are working to identify and advance norms of behavior in cyberspace. The norms and confidence-building mea-

asures proposed by the 2013 and 2015 UN GGE, while subsequently endorsed, lack enforcement mechanisms, making adherence voluntary. Without international consensus on cyber norms, the risk of cyber conflict and escalation increases as states continue to use cyber capabilities to achieve economic and geopolitical goals.

Scenarios: 3, 4

- A. Tumkevič, “Uncertain Security Community,” *Journal of Information Warfare* 17, no. 1 (2018): 74–86, <https://www.jstor.org/stable/26504130>.
- Andrew Futter, “‘Cyber’ Arms Control Will Probably Be Quite Different from the Nuclear Realm,” What Does Cyber Arms Control Look Like? (European Leadership Network, 2020), 3–5, JSTOR, www.jstor.org/stable/resrep24727.5.
- Patryk Pawlak, Eneken Tikk, and Mika Kerttunen, “Cyber Conflict Uncoded,” (European Union Institute for Security Studies (EUISS), 2020), JSTOR, <https://doi.org/10.2815/58797>.
- Kenneth B. Moss, “Challenges to International Regulation of Cyber Technology at War” (Danish Institute for International Studies, 2014), JSTOR, <http://www.jstor.org/stable/resrep13111>.

The Vulnerability of the Global Supply Chain

The complexity of the global supply chain has increased supply chain risks and potential points of failure. Third-party risk has become an increasing problem, especially in the technology sector, as manufacturers did not always know the origin country of manufacturing components. Decision-making processes in supply chains overemphasized efficiency but did not adequately consider rising security threats in the global landscape. In the last decade government organizations and private companies have dealt with increasing cybersecurity breaches and loss of intellectual property from supply chain risks.

Scenario: 1

- Ravi Sarathy, “Security and the Global Supply Chain,” *Transportation Journal* 45, no. 4 (2006): 28–51.
- Chang Won Lee and Gregory W. Ulferts, “Managing Supply Chain Risks and Risk Mitigation Strategies,” *North Korean Review* 7, no. 2 (2011): 34–44.

- Irvin Varkonyi, “DOD, Global Supply Chain and Supply Chain Talent Shortages,” *Defense Transportation Journal* 69, no. 3 (2013): 25–28.
- Tobin E. Porterfield, John R. Macdonald, and Stanley E. Griffis, “An Exploration of the Relational Effects of Supply Chain Disruptions,” *Transportation Journal* 51, no. 4 (2012): 399–427, <https://doi.org/10.5325/transportationj.51.4.0399>.

COVID-19

Speeding the Transition into Reliance on the Digital World as a Place for Human Interaction

COVID-19 greatly accelerated digital transformation, forcing individuals, governments, and organizations to rely on technology to continue day-to-day operations, business functions, and the delivery of critical services. The need for digital alternatives forced governments to lower restrictions on innovation and data usage to enable expansion of digital services, like telemedicine, and integration with applications like Zoom, Microsoft Teams, and other digital tools. Increased reliance on digital is propelling advances in data and network infrastructure to meet capacity needs.

Scenarios: 1, 4

- Till Contzen, “Increase Resilience through Digitization,” *Deloitte*, July 28, 2020, <https://www2.deloitte.com/global/en/pages/legal/covid-19/accelerate-digitization-increase-resilience.html>.
- D. Horgan et al., “Digitalisation and COVID-19: The Perfect Storm,” *Biomedicine Hub* 5, no. 3 (2020): 1–23, <https://doi.org/10.1159/000511232>.

Increased Reliance on Work from Home

COVID-19 transformed the labor force as workers transitioned to remote work during quarantine measures. In the U.S., 42 percent of the labor force reported working from home. Employees and organizations now rely on application services and tools for remote work and collaboration to continue business operations. An increasing number of corporations are developing plans to offer remote work options beyond the pandemic.

Scenarios: 1, 4

- Matthew Dey et al., “Ability to Work from Home,” *Monthly Labor Review*, 2020, 1–19, <https://www.bls.gov/opub/mlr/2020/article/pdf/ability-to-work-from-home.pdf>.
- “Is the Office Finished?,” *The Economist*, September 10, 2020, <https://www.economist.com/leaders/2020/09/12/is-the-office-finished>.
- Matt Clancy, “Remote Work Is Here to Stay,” *The Economist Intelligence Unit*, May 27, 2020, <https://eiuperspectives.economist.com/technology-innovation/remote-work-here-stay>.

APPENDIX 3: SCENARIOS

Scenario 1: Political Coercion via Municipal Attacks

Adversary: Iran, Enabled by Russia

Industry Focus: Electric Grid and Transportation Network

Key Challenge Drivers:

- Thread 1: Cybersecurity progress among Federal, State, and Local governments has been slow as resources are stretched thin in an economy weighed down by a slow COVID recovery.
- Thread 2: “Technology Nationalism” has created a concentration of vulnerabilities as nations seek to only utilize their own components.
- Thread 3: Critical systems in the United States, especially electricity and transportation, are dependent on IoT to function as they implement automation.

Key Adversary Actions:

- Iranian hackers discover a vulnerability, allowing them to access the unified central management system controlling the electricity grid.
- Iranian hackers correctly guess that the growth in technology nationalism has led the same developers who developed the “smart” grid management system to also create the “smart” transportation system: the Iranian hackers exploit the same vulnerability.
- Iranian Revolutionary Guard Corps (IRGC) actors target ISPs by bricking network switching gear resulting in Internet outages.

Scenario 2: Rise of a Global Tech Competitor

Adversary: China

Industry Focus: Manufacturing and Logistics, Artificial Intelligence, Media

Key Challenge Drivers:

- Thread 1: China has achieved technological self-sufficiency and leadership in many realms.
- Thread 2: China, through provision of niche 5G as well as IoT technologies, has penetrated the supply chain of specific sectors and can disrupt U.S. shipping and logistics.
- Thread 3: The U.S. has increased its dependence on artificial intelligence and machine learning (AI/ML) in a variety of economic sectors including health, finance, transportation, and media.
- Thread 4: Disinformation and manipulated media has become prevalent in social media platforms. Foreign adversaries consistently wage disinformation campaigns at a volume that social media take down the majority of false content.

Key Adversary Actions:

- Chinese establish remote access to smart port terminals through a satellite pushed update to smart port base stations provided by Chinese firms.
- PLA hackers disrupt factories via well-hidden backdoors in Chinese-owned centralized management applications for smart factories. The backdoors are hidden through unmapped interactions in the IoT environment.
- PLA hackers manipulate the AI models utilized to understand virus propagation. Providing different and inaccurate predictions slow down the development of a new vaccine.

- PLA conducts large-scale disinformation campaigns, using advanced deep and shallow fakes portraying a failed government response to the crises. Social media struggles to take down the fake content, and republishing is rampant.

Scenario 3: Digital Underground Enables Criminal Activity and Financial Attack

Adversaries: North Korea and Criminal Groups

Industry Focus: Financial Sector and Cybersecurity Industry

Key Challenge Drivers:

- Thread 1: Attackers continue to improve attacks and steal money from a wide range of payments systems leveraging sophisticated tools now widely accessible to both state and organized criminal actors.
- Thread 2: Crypto currencies and exchanges grow in use and technical ability to allow secure transactions.
- Thread 3: Aggregation of security solutions into managed security service providers (MSSPs) has concentrated vulnerabilities. MSSPs focus on providing compliance and protection against legal action given their market incentives rather than ability to defend specific clients against targeted attacks.
- Thread 4: Cloud-based vulnerabilities and associated exploits have grown as the financial sector increasingly moves services and supporting remote work forces rely on the cloud.

Key Adversary Actions:

- North Korean threat actors compromise a major MSSP and leverage the remote management tool to infiltrate a major financial sector institution. Once inside, the attackers drop a wiper worm that is able to self-propagate through the network utilizing the new cloud exploit. As other financial institutions send information requests to the infected bank, they also become contaminated with the wiper.

Scenario 4: Domestic Violent Extremism

Adversary: Domestic Extremist Groups

Industry Focus: Media and Major Technology Providers

Key Challenge Drivers:

- Thread 1: Increasing movement of society to cloud-based services, remote work, and use of IoT make those requiring cloud and core network dependent resources vulnerable to cyberattack and disruption.
- Thread 2: Unclear responsibilities and competing priorities for media in reporting on digital domestic extremism and coordination with government to help with digital public safety
- Thread 3: Roles of federal/state/local authorities are unclear in responding to cyberattacks emanating from domestic sources that impact national and economic security.

Key Adversary Actions:

- Hacktivists exploit weak identity management to target law enforcement networks. Hackers deface and disrupt law enforcement websites and networks, crippling a response to the domestic extremists.
- Hacktivists exploit vulnerabilities in weak APIs for remote health services to disrupt healthcare.
- Hacktivists utilize a combination of built-in network protocols necessary for remote work to create massive, amplified DDoS attacks against critical nodes in cloud infrastructure, disrupting smart cities, including government services with a focus on law enforcement.

APPENDIX 4: WORKSHOP FINDINGS

Workshop 1

State and Municipal Response

Identified Challenges:

- Filling capacity in crises requires overlaying/building in talent according to documented talent requirements rather than simply providing capacity from the outside
 - ◇ Must be done at scale and with sufficient endurance and be operable even if funding dries up during crises
- Difficulty of balancing the trade-offs between searching for other vulnerabilities and immediate remediation efforts
- Need to carefully filter out less useful and potentially dangerous volunteers to make volunteer assistance productive and not add another source of vulnerabilities or threats

Identified Obstacles:

- Lack of investment in workforce/talent building for both proactive resiliency building as well as key crisis response skill sets, situational awareness, assessment, incident analysis/forensics, and network/systems build. Need to acknowledge what skill sets are needed at what levels and which organizations/authorities have the knowledge and resources to establish proper response capabilities.
 - ◇ There is an existing shortage of people capable of leading coordinated response efforts. This causes institutional challenges in creating this capability as there are few people able to define response requirements

- Lack of highly efficient funding mechanisms for response preparation and/or sustained responses
 - ◇ States and municipal jurisdictions face legal constraints in attempting to fund cybersecurity action (OSD does not view activity under 32 U.S.C. 502(f)) as a permissible activity for Guard units to receiving Federal funding)
- Lack of identified structures and business rules that support collaboration, from either the public or private sectors
- Lack of understanding around the concept of “Combined Cyber Incident Response (CCIR)”
- Lack of common framework for state and local governments to request capabilities they need and that providers at higher levels can assign people and team that fit the requested need and situation
- Lack of framework to bring in private sector talent to buffer and help state and local responders

Recommendations:

- Extend Stafford Act or create cyber-specific funding mechanism, such as a Cyber Response and Recovery Fund, that allows for flexible response to crises, contains coordination stipulations, includes a “preparedness framework,” and is well defined in terms of how it would be used
 - ◇ Consider the full range of sectors potentially affected, the unique geography of cyber response, and regulatory concerns and legal liabilities for the private sector
 - ◇ Cyber Response and Recovery Fund should be authorized to provide resources to public and

private sector organizations, including at the state and local level

- ◇ The Fund should be specific enough that in crises, cyber response does not compete with response to natural disaster or health crisis, and broad enough that states with an already adequate system do not have to change
- ◇ Funding act has integration with the private cybersecurity sector as well as critical infrastructure and IT groups
- Create a minimum core capacity that states must meet through marshaling the National Guard and other resources in the event of cyber incidents
 - ◇ States in coordination with municipalities should set baseline cyber training standards with the option to build up more advanced capability for diversification of capabilities
 - ◇ Flexibly account for states' unique strengths as well as regional alliances, and allow higher-order expertise to be easily shifted in crises
 - ◇ If a core capacity cannot be feasibly distributed across municipal levels, have a common system for identification of vulnerabilities and agreed upon threats
- Treat key private sector players as national security partners fully engaged in preparation and readiness to defend the nation, and take strengths of both sides into account in collaborative ventures
 - ◇ Require Joint Interagency Task Force (JI-ATF)-like structured joint processes for integration into planning, common operating picture and response decisions, and forming public-private cooperation mechanisms
 - ◇ Increase coordination with and utilization of Office of General Counsel's attorneys, identify and incorporate relevant existent solutions to solve future issues, and avoid executives having to make difficult security decisions
 - ◇ Establish clear limits on private sector actions: participation in these joint efforts does not authorize otherwise illegal activity (i.e., "hack back")

Communication Risks

Identified Challenges:

- Information and intelligence sharing, and response planning, is difficult and unclear between the public and private sectors encounter
 - ◇ Private sector tends to possess knowledge of technical intelligence but lacks insight and situational awareness of the big picture, which the Federal government has. Municipalities often find themselves stuck in between with technical intelligence provided by private sector vendors and some intergovernmental channels providing a limited amount of big picture intelligence
- Difficulty in communicating systemic cyber risk to business and government leaders
- Challenge in creating composite picture of risk of any given crisis in real time due to lack of joint communications and sharing
 - ◇ Challenge of bringing together different events in one operational picture as each breach and compromise is published as in independent event
- Even with high-fidelity sharing, intelligence gaps and uncertainty will still remain

Identified Obstacles:

- Lack of organic cooperation between federal, state, and local governments leads to poor communication and information sharing
- Lack of dedicated lines of communication, preexisting organizations, and planning to enable rapid communication in event of a crisis
- Existing legal barriers (e.g., NDAs, paperwork, etc.) hinder vendors from responding rapidly in the event of a crisis
 - ◇ There needs to be a mechanism to default offer full protection from legal recourse for any information devolved to better enable a response in a timely manner

Recommendations:

- Create dedicated cyber coordinator role at local, state, and federal levels
 - ◇ At the Federal level, the housing entity should have 30–40 positions dedicated to coordinating with State and major municipality cybersecurity coordinators (preferably located in their regions)
 - ◇ Each State and large municipality should have a dedicated cybersecurity coordinator position
- The coordinator position responsibilities:
 - ◇ Collaboration and integration of cyber response capabilities across levels of government and across public and private sector
 - ◇ State cyber coordinators work with CISA or a CISA state appointee to improve communication and planning between federal and state levels
 - ◇ Planning for crisis mobilization
 - ◇ Management and delegation of incoming resources during cyber crisis response
 - ◇ National coordinator's duty includes helping advocate for structures and investments: creating an organization for coordinators to congregate, including private sector partners
 - ◇ Cyber coordinators ensure that there is a version of the cyber funding mechanism that is tailored to the state or local level
- Increase integration of private sector into government by enabling private sector to plug into government structures; have private sector liaisons/coordinators to work with government
 - ◇ Build collaboration centers; FSR/NCCIC can be used as case studies
 - ◇ Create competitive funding, subsidies, or legal incentives for private sector to collaborate with government to incentivize public-private collaboration
- Create resilient intelligence sharing mechanisms be-

tween public and private sectors and between federal, state, and local governments

- ◇ Need to create shared command and control capabilities for information sharing, including need to include operational plans and coordinating action
- ◇ Need to include state, local, and private stakeholders in the intelligence cycle consistently, not just in time of crisis

Mobilization

Identified Challenges:

- Difficult and costly to sustain capability at a high level of readiness over the long term or while facing a shortfall in capacity
- Unclear if the assets and resources for incident response currently available at the federal, state, local, and industry levels are adequate and able to scale
 - ◇ Need to identify response capabilities in absence of USCYBERCOM and National Guard
 - ◇ Need to identify other potentially useful federal resources that can be deployed more locally
- Shortage of experienced and capable personnel will be exacerbated during a crisis due to competition for those scarce resources

Identified Obstacles:

- Lack of layers of trust between levels of government and the private sector
- Lack of common situational awareness and lack of common operating picture
- Lack of a common operating model
 - ◇ Model/framework needs to be more than infrastructure, but exercised
 - ◇ Need to have Cyber Response Group (CRG) and teams ready in advance

Recommendations:

- Cyber coordinators and associated organizations must map existing capabilities and plan for sustained resource costs associated with maintaining full crisis response mobilization for sustained period
 - ◇ Need to integrate and account for resources outside the U.S., especially that of U.S. allies, in advance of crisis for accurate planning and response management
- Prepare necessary legal agreements, and have them ready for rapid execution in the event of a crisis
- Organize joint exercises and training between private, public, state, local, and federal levels. Must sustain activity for cooperation mechanisms to ensure smooth operations during crisis
 - ◇ Nodes play a key role in connecting into the private sector by being legally and structurally prepared to quickly integrate government response with the correct identification of private sector capabilities
- Create situational and state-dependent communication and resource pathways between states and municipal/local levels for states in which this is lacking so that states with legal jurisdiction over incident response are working with local law enforcement and private enterprise
 - ◇ Form a general parameter of states understanding how to best support the local levels on top risks

Workshop 2

Decoupling and Tech/Supply Chain Risk

Identified Challenges:

- Effective decoupling (both in terms of security risk management and avoiding unnecessary costs) necessitates increased information exchange between government and affected organizations
- Balancing national security perspectives with business considerations, i.e., cost of an attack versus cost of market loss

- ◇ Need to forecast and consider difficulties for long-term losses and gains from decoupling besides immediate economic inefficiencies and security efficiencies

- Difficulty in incentivizing private sector to invest in operational readiness

Identified Obstacles:

- Lack of forecasting of long-term gains/losses in the event of decoupling
- Lack of information exchange between government and affected organizations
- Lack of collaborative approaches for U.S. government to help private sector mitigate the high costs and changes to business models that will result from decoupling
- Lack of cooperation in building security measures for sectors with less resources
- Lack of incentivization for the private sector to work with public sector:
 - ◇ No assignment of roles and who sets rules in different key industries
 - ◇ Consideration of differentiating sectors' degrees of entanglement/decoupling
 - ◇ Companies may choose to not disclose supply chain vulnerabilities/attacks

Recommendations:

- Sectors develop common standards for identifying and reporting presence of:
 - ◇ Methods that can organically develop within the private sector is ideal; Protected Critical Infrastructure Information (PCII) standards, while for a different purpose, provide an industry-driven model for development
 - ◇ Create agile contractual enhancements that incorporate supply chain vetting and actions to remove risk by contracted parties; require security reviews/sign-offs
 - ◇ Develop crisis reporting and impact assessment capability for discovered supply chain

vulnerabilities/emerging risks in a crisis

- ◇ Use NIST or other players to build best practices that can protect against sensitive and/or personal data vulnerabilities
- Create measures to motivate private sector to develop resiliency and standards
 - ◇ A combination of both incentivization and regulation to create operational resiliency and better standards in conjunction with the government
 - ◇ PCI or strengthening incentives for supply chain risk management by fostering private sector lead developed approaches (e.g., PCI) with government assistance (encouragement/fund/NIST process activated)
 - ◇ Marshall high-level cybersecurity experts to communicate data and other vulnerabilities to powerful yet still-unregulated companies
- Require defense for supply chain and embedded devices in the event of a crisis
 - ◇ Align funding with supply availability, use R&D investment/AI/ML to improve functionality testing, and shift to more general-purpose computing devices
 - ◇ Government departments can lean on FFRDCs/UARCs to underpin their regulations and decisions toward critical infrastructure readiness and security
 - ◇ Utilize broad legal definition of critical infrastructure to increase collaborative level between government and potentially vulnerable hubs
 - ◇ Use regulation or laws to encourage companies to extend supply chain responsibility down to sub-suppliers for a more secure supply chain

AI Vulnerabilities

Identified Challenges:

- Securing data sources for AI systems—as reliance on AI increases, greater data protection will be required

- Transitioning to cloud is unmapped and unregulated, creating high risk and increased vulnerabilities

Identified Obstacles:

- No definition of government's role during or after an attack on the cloud or AI in the private sector
- Lack of contingency planning: balancing continuity with data privacy regulations
- Incidentally creating locus for attacks by shifting to the cloud

Recommendations:

- Make cloud a critical national asset, similar to telecom and AT&T; develop regulatory and collaborative structure for Cloud
 - ◇ Use intersectionality between cloud providers, data providers, and health/data tracking sector to tie together different sectors into a new wing of critical infrastructure
 - ◇ In the event private sector organizations lack adequate cybersecurity capabilities for the cloud, create mechanism so cybersecurity experts/NSA can intervene and manage any cloud-based security vulnerabilities
- Develop improved technology and implementable integrity checks to respond at machine speed for data integrity challenges
 - ◇ Create measures for in-the-moment requirements
- Build capacity for backups in the event of a crisis; could use regulators/incentives
 - ◇ Could utilize an environmentalism model to force companies to decrease risk with how they store/save data
 - ◇ Account for the backups/backup companies being implicated in attacks
- Use holistic data/minimization regulations such as DHS/HHS/FFIEC regulations to minimize vulnerabilities and risk
 - ◇ Secure data sources for AI systems could

potentially be handled by sector-specific players to account for the greater data usage and data protection that increased reliance on AI will require

Public Confidence and Trust

Identified Challenges:

- Challenge in combatting disinformation that could amplify a cyber crisis
 - ◇ Ensuring the media is held to an appropriate standard in validating information
 - ◇ U.S. lacks implement trust evaluation mechanisms for citizens to judge the validity of information in media channels and organizations
- Taking steps to improve trust between traditional media, levels of government dealing with media, and social media
 - ◇ Account for trust issues if information comes from government Computer Emergency Response Teams (CERT)
 - ◇ Account for decreased trust in FDA/CDC; restoring trust in government institutions still important; can start from within
 - ◇ Consider free-speech principles, especially in terms of attribution

Identified Obstacles:

- Lack of trust and collaboration mechanisms for crisis communications between government and social media platforms and influencers
- Cybersecurity's lack of an FDA/CDC equivalent erodes trust when government issues cyber news/reports; progress being made—CISA/FBI current reports—need to reinforce trend
- Need to address information gap and different incentives for describing evolution of events in a cyber crisis between cybersecurity teams and journalists regarding what attacks, disruptions, and impacts are occurring and their significance

Recommendations:

- Improve media sources' awareness/accountability by employing fact-checker or bias-evaluator tools; use FCC to clarify expectations for public broadcasters
 - ◇ Encourage cybersecurity officials to cultivate relationships with traditional media organizations and reporters to build trust; ensure good, unclassified information has a channel out of government; and decrease information gap
- Create independent media regulatory organization to build trust between government, media, and the public
 - ◇ Would need to collaborate across competitive industries
- Create an approach to put content moderation measures in place during crisis between government and social media companies
 - ◇ Need to understand if/when governmental emergency powers will be invoked; recommend legislative updates/changes as needed (e.g., 1934 Communications Act)

Workshop 3

Cybercrime

Identified Challenges:

- Issue within financial sector of tension between supplying consumers with rapid transaction times and addressing security needs
- Challenge of finding healthy medium between key private companies sitting in on the common operating picture versus only receiving briefings after criminal events have already occurred
- Targeting cryptocurrency necessitates identifying the natural set of private/public players for the most effective collaboration
- Cryptocurrency requires a balanced approach to operational intervention between law enforcement and national security

- Defining impactful criminal activity and when criminal becomes systemic/national security issue—little identification/definition when that boundary is crossed and how to respond

Identified Obstacles:

- Lack of clarity or standards on what constitutes a sanitized and safe environment after a compromise has taken place
- Lack of common framework for when and how to reconnect to previously compromised parties
- Tension between fast transaction times and security needs within the financial sector
- Gap in decision making and jurisdiction: if Cyber Commands begins proactively targeting cybercrime, who has the proper authorities?
- Lack of framework for role of regulators and government in declaring an environment safe after being compromised
- Limitations of current DHS/Cyber Command/CISA collaborative structure in supplying resources for cyber response and proactively raising national funding up to a necessary level

Recommendations:

- In developing operational plans for moving forward, nodes should clearly delineate between what is criminal behavior and what is national security for both pre-event and post-event collaboration
- For an operational structure with maximum flexibility, designate nodes spanning borders and sectors that in turn create public-private partnered threat cells to address any given crisis
 - ◊ Nodes need full capabilities to bring in systemically important players to develop partnerships, understand different perspectives before crises, and enhance operational collaboration
 - ◊ Nodes run scenarios or use data garnered by threat cells to assimilate and house results to act as a baseline for future response, and distribute these to nodes across other regions and sectors
 - ◊ Threat cells bring together law enforcement

agencies, platform providers, telecommunications network companies, cybersecurity providers, FinTech start-ups, and emerging critical infrastructure providers (cloud)

- Regulators contribute to crisis response by removing obstacles during crisis rather than by guiding response
- Long-term, explore creation of stand-alone cybersecurity/critical infrastructure agency with goals of halting deemphasis on cyber and creating more support and capacity for Cyber Command/other forces to focus on more than one issue at a time

Cryptocurrency

Identified Challenges:

- Need to account for targeting “nefarious” exchanges while not affecting “good” exchanges and the inherent possible side effects
 - ◊ Need to build response for disrupting actors using technical infrastructure in countries friendly to them
- Possible Balkanization of the financial sector if tranches of small and medium financial institutions are incidentally interacting with criminal crypto exchanges, unwittingly aiding in crypto money laundering

Identified Obstacles:

- Lack of a mechanism to determine who is responsible for regulating cryptocurrency and stop criminalization of cryptocurrency
- Gap in representation of small and medium financial institutions creates a vulnerable tranche within sector
 - ◊ Need to identify if ISAC/FSARC model will work for small- and medium-sized banks or needs to be replaced

Recommendations:

- U.S. National Security community needs to recognize the security dimensions of cryptocurrencies in AML, counterterrorism, and sanctions bypassing, motivating and incentivizing regulators to exert pressure on entities aiding nefarious crypto activity (e.g., Fintech companies)

Ransomware

Identified Challenges:

- Difficulty of differentiating roles and priority between criminal justice or national security in ransomware attacks
- Capability gap between defensive response and offensive ransomware as a service
- Defensive response cannot keep up with the developments
- Coordinating agency action when it is unclear who the victim entity is (MSSPs, impacted banks, impacted providers, etc.) in the interaction causes myriad issues
- Difficulty of dealing with political and economic pressure to put affected institutions back online before a threat has been dealt with properly
 - ◇ Private sector is incentivized to pay for their own recovery and resume operations as rapidly as possible
- Possible Balkanization of the financial sector if tranches of small and medium financial institutions are cut off from larger institutions due to contamination fears

Identified Obstacles:

- No existing structure or playbooks that adequately address the dynamic environment of competing priorities from a variety of affected entities that ransomware presents
- Lack of cohesive picture on how private sector can assist public sector with tracking ransomware actors and how human capital that can orchestrate joint ransomware responses can be identified

Recommendations:

- Streamline exchange functions between private sector and government in ransomware attacks to create cohesion and familiarity and avoid arbitrage
 - ◇ Ensure private and public sector create direct and ongoing pipelines for direct participation in service exchanges to allow for more

collaborative response (e.g., private sector participation in NCIJTF, Cyber Command through rotational program, etc.)

- ◇ Develop mechanisms to shield private sector from commercial – understand their platforms and assets
- Co-create playbooks between private and public stakeholders to orchestrate joint cohesive ransomware response

MSSPs

Identified Challenges:

- Difficulty of incentivizing MSSPs to keep up with evolving threats and reporting the threats that they face
 - ◇ Unclear whether mid-sized MSSPs servicing downstream clients in the market provide sufficient protective value from criminal elements with advanced capabilities
 - ◇ Unclear if market power of the financial sector can make the MSSP model become more responsive to emerging threats
- Difficulty in identifying role of government and regulatory authorities in supervising MSSPs and ensuring their safety
 - ◇ Identifying what MSSPs are responsible for and how far their responsibilities reach
 - ◇ Difficulty in ensuring the safety of MSSPs themselves as a threat vector due to their connectivity to institutions

Identified Obstacles:

- Lack of liability structure when MSSPs fail to provide their advertised service
 - ◇ Need to account for the danger of regulating liabilities of MSSPs without it becoming a paperwork drill—must not overregulate; must incentivize to be proactive and increase capabilities against targeted attacks rather than achieve standards

- Lack of market incentivization for MSSPs to develop advanced security capabilities
 - ◊ SMB's, particularly in financial sector, contract MSSPs due to regulatory pressure; mid-sized MSSPs have little motivation to develop capabilities past their client's demand
- Lack of liability for MSSPs as a vector attack

Recommendations:

- Form, relaunch, or maintain existing collaborative and communicative umbrellas between operators and decision makers with the goal of forging relationships between MSSPs and public sector
 - ◊ Find or create mechanisms to ensure MSSPs are linked to the critical nodes in the cyber ecosystem
 - ◊ Designate major MSSPs as nodes and integrate them into system

Workshop 4

Pursuing Action against Domestic Threat Actors

Identified Challenges:

- Execution difficulties stemming from conducting cybersecurity operations while simultaneously taking law enforcement actions to apprehend perpetrators
- Ancillary problems arising from law enforcement capabilities being hindered or affected in an attack could create a ripple effect
 - ◊ Consequent priority to bring basic policing and law enforcement services back online could divert resources and energy from immediate defensive efforts. Must account for possibility of malicious actors launching cyber actions to protect physical activities or launch physical activities to distract from cyber activities

Identified Obstacles:

- Legal barriers to domestic intelligence gathering beyond FBI/law enforcement

- ◊ Lack of capacity for domestic intelligence gathering as most U.S. intelligence capabilities focused and/or situated abroad
- ◊ Lack of established legal framework to overcome legal constraints on domestic intelligence gathering for emergency situations

- Lack of precedent and clarity on how private sector stakeholders would receive situational awareness related to impacts of cyberattacks and projected next actions by government in a cyber crisis generated by domestic threat actor
- Lack of a legal structure enabling municipal law enforcement to receive applicable cyber intelligence from federal sources

Recommendations:

- Provide mechanisms for law enforcement agencies to collect sufficient information in the case of domestic cyberattacks
 - ◊ Facilitate intelligence exchange between federal and municipal law enforcement and private sector to forge a more proactive and efficient common approach
- Create a schema to enable a trust structure between public and private sectors to address gaps in necessary information sharing by government with private sector outside of those currently covered (extremist content, etc.)

Collaboration

Identified Challenges:

- Overarching challenge in government's coordination of:
 - ◊ Roles and responsibilities for response actions due to a granular understanding of differing capabilities/skill sets provided by a range of governmental actors at federal, state, and local level as well as private sector
 - ◊ Understanding capability gaps that need to be filled for different situations and which actors are best suited for the crisis response at hand

- Uncertainty of roles and responsibilities depending on collaboration as a federal-first process (e.g., law enforcement) or a federally supported process (e.g., asset response)
- Challenge of ensuring that sustained public-private operational collaboration will occur as normal course of business and not solely during focused events/potential high-risk situations (e.g., Trickbot and elections)
- Reluctance from private sector to collaborate when navigating highly partisan political contexts and diverse constituent concerns

Identified Obstacles:

- Lack of municipal readiness plans in the vein of business continuity plans across various industries
- Lack of legal structures available to provide ISPs and cloud providers with an adequate authority to collaborate in taking action to support crisis response
- Lack of best practices in how to educate private sector companies that increasingly rely on the cloud maintaining strong cloud-based cyber security capabilities/practices

Recommendations:

- Create a clear, focused legal mandate for government's access to information sharing
 - ◇ Provide clear authority for Federal agencies to gather necessary information from impacted private sector organizations during a cyber crisis to provide situational awareness
 - ◇ Empower appropriate private sector actors to take action by:
 - Correctly identifying which companies can disrupt the most pressing activities
 - Leveraging a CTA-like interlocutor to ease burdens on attaining otherwise scarce information
- Encourage private sector to participate more in information transfers
 - ◇ Specifically delineate what information is and is not competitive advantage

- ◇ Assuage globalized companies' concerns; expect participation in only information transfers that are neither adversarial toward other countries nor a violation of international law
- ◇ Incentivize companies to provide attack data from suspected breaches, not only confirmed breaches
- ◇ Enable companies to feed forensic information back to collaborative and government entities for identification, attribution, and dissemination

Common Operating Picture

Identified Challenges:

- Federal government challenged to find best ways to assist in delegation and resource management when needing to account for:
 - ◇ Different levels or agencies of law enforcement
 - ◇ Differences in law enforcement at state and local levels
- Difficulty in achieving ground truth in any given operational picture with rampant misinformation or disinformation
- Private sector needs to be able to plug into a common operational awareness picture so that elements of response that have corporate effects will be informed

Identified Obstacles:

- If traditional media or communications tools became untrustworthy or compromised, law enforcement would deal with a lack of communications dominance
- If commonly used operational tools are impacted in an attack, the usage of outdated tools would create numerous security vulnerabilities
- Lack of clarity on:
 - ◇ Which entity coordinates information sharing between public/private sectors
 - ◇ How the government or cloud service providers would push information to local teams in an emergency event

Recommendations:

- Ensure that nodes/threat analysis cell structure can integrate with joint task force and other response infrastructures that do not duplicate and have highly integrated data flows to enable a common operating picture
 - ◇ Involve DHS/FBI/CISA in tabletop exercises and operational scenarios with key state, local, and private sector players to create ready-made playbooks for each organization in event of crises
 - ◇ Study evolution of the NCIJTF to examine different types of operational collaboration
 - ◇ Examine NCFTA lessons regarding legal authorities for coordination and action
 - ◇ Ensure that preexisting task forces (Secret Service, FBI, etc.) collaborate, share resources, and make budgets readily available

Trust and Public Confidence

Identified Challenges:

- Difficulty in building public trust and confidence without getting into First Amendment questions and debates
 - ◇ Challenge in defining line between freedom of speech and censorship
 - ◇ Challenge in domestic intelligence gathering versus privacy rights
- Need to account for different permutations of trust across different levels of relationships
- Prevalence of misinformation and disinformation creates increased importance of clear communications and necessitates that words and actions not further erode trust
 - ◇ Challenge in limiting generation and spread of disinformation clogging lines of communication en masse
- Difficulty in cohesively implementing civics education with digital literacy

Identified Obstacles:

- Lack of clear methods and initiatives to shift the optics and messaging on cybersecurity to the general public to create an increasingly positive impression of cyber operations
- Improvement necessary for clear communications on operational collaboration activities, as backwards press releases (e.g., Cyber Command around Trickbot) have driven distrust in both government and corporations
- Lack of dedicated resources for digital education and literacy

Recommendations:

- Increase transparency and bring in observers from the public (cyber nonprofits) and commercial sectors to allow government to build back and improve public trust and validation
 - ◇ Start to build fundamental trust in existing partnerships through joint action and integration—joint operations (i.e., Trickbot take-down), exercises, joint programs, reporting
 - ◇ Report on positive developments in cyberspace including education programs
- Create structure for increased transparency into the media cycle to organically evolve from within private sector
 - ◇ Verifying sources and requiring fact checks
- Provide resources to joint operating structure to create cyber education and digital media literacy programs
 - ◇ Incentivize the promotion of awareness campaigns for the public

APPENDIX 5: SOLARIUM COMMISSION AND NDAA OBSERVATIONS

The Task Force views the recent U.S. Cyberspace Solarium Commission report and the cybersecurity measures approved in the 2021 National Defense Authorization Act (NDAA) as positive steps toward improving national cyber readiness. We particularly commend the Solarium Commission's focus on promoting operational collaboration with the private sector and welcome the inclusion of some of these measures in the final NDAA.

One Solarium Commission recommendation passed in the NDAA establishes a National Cyber Director and an associated Office of the National Cyber Director (ONCD) within the Executive Office of the President. We believe that the National Cyber Director position is a critical role that will improve operational collaboration and national cyber operational readiness. The designation of roles, particularly for defensive operational planning, operational response, and coordination with the private sector, will be a key initiative for the ONCD to undertake. For the ONCD to properly achieve its mission it must be well staffed and resourced.

- The establishment of the Joint Cyber Planning Office under CISA that explicitly engages both private and public sector entities closely maps to our concept of an operational response network. We hope that this office is allocated the proper resources and staff to undertake rapid development of efficient processes for deep collaboration with private sector stakeholders as full partners. We strongly endorse the concept of defensive operational plans and believe such plans must be aligned with identified and prioritized national cyber crisis contingencies.
- The creation of a Biennial National Cyber Exercise establishing a federal cyber exercise with the participation of federal, state, and private sector stakeholders is strongly supported. The

inclusion of the state and private sector levels is a strong step in building operational collaboration. The Task Force strongly recommends that the National Cyber Exercise also include municipal-level stakeholders and that the exercise includes a strong component focused on evaluating cyber response readiness considering defensive operational plans aligned to national cyber crisis contingencies.

The Task Force assesses that 2021 NDAA measures fall short in some critical areas that would strengthen operational readiness. In particular:

- The Task Force strongly supports the Solarium Commission's recommendation to codify a Cyber State of Distress tied to a Cyber Response and Recovery Fund. Such a fund would begin to remedy critical gaps in the lack of emergency resources in the case of a major cyber crisis.
- The creation of a Joint Collaborative Environment would also have greatly contributed to private public operational readiness. An integrated cyber center within CISA would also have provided strong operational gains in building operational readiness. The benefits of both these initiatives have been illustrated in great depth in the body of the Task Force's main report.
- The NYCTF also notes that numerous issues are left to further studies. These issues are often topics that have been studied before, such as the use of the National Guard in cyber response. The nation needs to focus on investing the proper resources to establish programs and roadmaps for building cyber operational readiness capabilities.

NOTES

1. New York Cyber Task Force, “Building a Defensible Cyberspace,” SIPA: School of International and Public Affairs. 2017. https://www.sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyber-space-WEB.PDF.
2. “Cyberspace Solarium Commission Report,” Cyberspace Solarium Commission, 2020. <https://www.solarium.gov/report>.
3. National Defense Authorization Act for Fiscal Year 2020, S.1790. <https://www.congress.gov/bill/116th-congress/senate-bill/1790>.
4. Aspen Cybersecurity Group. “A National Cybersecurity Agenda for Resilient Digital Infrastructure,” December 18, 2020. <https://www.aspeninstitute.org/publications/a-national-cybersecurity-agenda-for-resilient-digital-infrastructure/>.
5. In Appendix 5, we detail specific recommendations related to the Solarium Commission’s findings and the 2021 NDAA provisions on operational collaboration.
6. The Atlantic Council hosts the Cyber 9/12 Strategy Challenge, an annual cyber policy and strategy competition where students across the globe compete in developing policy recommendations to remediate a fictional cyber catastrophe.
7. While quantum computing has made major advancements and will likely become an influential technology in the future, Task Force members agreed that widespread usage of quantum computing by 2025 is highly implausible. Michael J. D. Vermeer and Evan D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*, Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3102.html.
8. Peter Schwartz, *The Art of the Long View: Paths to Strategic Insight for Yourself and Your Company*, Toronto: Doubleday, 1996.
9. The day after, methodology was used by RAND both in analyzing nuclear proliferation issues as well as emerging cyber issues in the 1980s and 1990s. We point you to the following report: Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, Santa Monica, CA: RAND Corporation, 1996. https://www.rand.org/pubs/monograph_reports/MR661.html.
10. “Announcing the Formation of the Analysis & Resilience Center (ARC) for Systemic Risk,” Business Wire, October 30, 2020. <https://www.businesswire.com/news/home/20201030005462/en/Announcing-the-Formation-of-the-Analysis-Resilience-Center-ARC-for-Systemic-Risk>.
11. “Cyberspace Solarium Commission Report,” Cyberspace Solarium Commission, 2020, p. 109. <https://www.solarium.gov/report>.
12. “National Security Telecommunications Advisory Committee,” Cybersecurity and Infrastructure Agency, 2021, <https://www.cisa.gov/nstac>.
13. Tom Burt, “New Action to Combat Ransomware Ahead of U.S. Elections,” Microsoft On the Issues, December 17, 2020. <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyber-threat-us-elections/>.
14. National Defense Authorization Act for Fiscal Year 2020, S.1790. <https://www.congress.gov/bill/116th-congress/senate-bill/1790>.



WHERE THE
WORLD CONNECTS

Cyber@SIPA

SIPA.COLUMBIA.EDU