THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem

September 3, 2019

TABLE OF CONTENTS

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION 1

1.1 Scoping and Charge 2

2.0 THE DESIRED END STATE 3

2.1 Factors Preventing the Desired End State 4
2.2 What the United States Government Is Getting Right 6

3.0 THE CHALLENGE 10

4.0 RECOMMENDATIONS 13

4.1 Senior Advisor to the President for ICT Resiliency 13
4.2 U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem. 15
4.2.1 Identify Stakeholders 16
4.2.2 Identify Desired Actions 17
4.2.3 Identify Missing Structures and Processes 24
4.2.4 Identify and Leverage the United States' Natural Strategic Advantages 27
4.2.5 Foster Stronger Cooperation Amongst Like-minded Nations 28
4.2.6 Advancing the Strategy's Goals 29

5.0 CONCLUSION 30

APPENDIX A: 5G CASE STUDY A-1

APPENDIX B: STRONG U.S. SEMICONDUCTOR INDUSTRY CRITICAL TO ICT RESILIENCY B-1

APPENDIX C: STANDARDS BODIES C-1

APPENDIX D: SUBCOMMITTEE MEMBERSHIP D-1

APPENDIX E: ACRONYMS E-1

APPENDIX F: GLOSSARY F-1

APPENDIX G: BIBLIOGRAPHY G-1

EXECUTIVE SUMMARY

Ensuring that the information and communications technology (ICT) that supports U.S. national security and emergency preparedness (NS/EP) missions is available, reliable, and trustworthy is one of the United States' greatest national imperatives. This was at the heart of the President's National Security Telecommunications Advisory Committee's (NSTAC) recommendation in its *NSTAC Report to the President on a Cybersecurity Moonshot* for the Administration to declare a national strategic intent to "Make the internet safe and secure for the functioning of Government and critical services for the American people by 2028."[1] The reliance of government agencies and critical service providers on untrusted products and services has serious implications for U.S. national security and must be addressed more strategically and comprehensively.

> The term ICT generally refers to technologies that provide access to information. In this report, the term is used to refer to information technology equipment, systems, and networks, as well as other network-capable devices, including mobile devices.

A priority concern associated with the critical reliance on untrusted technologies is that the reduction in the availability of trusted manufacturers from certain ICT markets has diminished the choices of those who operate U.S. NS/EP functions which, as discussed further in this report, includes national critical infrastructure. Looking to the future, the United States must foster an environment for trusted parties to create, develop, and invest in certain emerging technologies that could eventually become critical to NS/EP so as not to create unsecure dependencies on untrusted manufacturers.

Another key concern has been the inability of government and industry to effectively address the national critical reliance on untrusted technologies. The reliance problem is not new but has been growing for some time. The multi-disciplinary and multi-stakeholder nature of the problem has served as a barrier to effective response. There is consequently a need for a national focal point that cuts across national security, economic security, and innovation to ensure these communities are effectively working in concert towards a common set of priority goals.

The United States requires a whole-of-nation approach to ensure that trusted manufacturers remain in key markets and to create the conditions that foster American innovation in key areas. This whole-of-nation approach must include a holistic national strategy and a dedicated White House position to coordinate the development and implementation of that strategy across U.S. federal departments and agencies (D/A), the critical infrastructure provider community, and the broader innovation community.

[1] NSTAC, *NSTAC Report to the President on a Cybersecurity Moonshot,* (Washington, DC: DHS, November 14, 2018), 2018 NSTAC Publications, https://www.dhs.gov/publication/2018-nstac-publications-0.

Defining NS/EP

The NSTAC considers NS/EP to mean the national security agencies, emergency preparedness organizations, and the critical sectors. Traditionally, NS/EP may have been considered to mean U.S. national security agencies and emergency preparedness organizations. However, today national security agencies and emergency preparedness organizations rely on many products and services provided by businesses such as banking, utilities, healthcare, and transportation. These are now referred to as the critical sectors both because of the role they play in national defense and security and their criticality to the day-to-day functioning of society. In 2013, Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, identified 16 critical sectors. These sectors provide critical services to society. The NSTAC equates these with the National Critical Functions (NCF) that were recently identified by the Department of Homeland Security. Throughout this report, the term NS/EP-critical ICT is used and means, "ICT that is depended on by the national security agencies, emergency preparedness organizations, the critical sectors and providers of the NCFs."

Key Recommendations: Senior Advisor to the President on ICT Resiliency (*Section 4.1*)

To address the urgent problem of critical reliance on untrusted technologies, the NSTAC recommends that the President create the position of Senior Advisor to the President for ICT Resiliency (Senior Advisor) who will report directly to the President. The purpose of the creation of the position of Senior Advisor is to more tightly coordinate the strategy and policy generating elements of the White House on matters relating to ICT resiliency and innovation which will flow down to operational activities of the D/As. The Senior Advisor should be empowered to lead the Nation in the development and implementation of a national policy and strategy on advancing ICT resiliency and fostering innovation. This will be accomplished in close coordination with the National Security Advisor, the Director of the National Economic Council, the Director of the Office of Science and Technology Policy, the U.S. Trade Representative, the heads of relevant D/As, and private sector stakeholders.

The recommended authorities of the Senior Advisor include the ability to convene and/or task the Executive Branch and the ability to convene and coordinate with non-government partners, leveraging existing processes already established by federal agencies and federal advisory committees, to include leaders from the manufacturing and innovation communities, owners and operators of critical infrastructure, and academia. The Senior Advisor will be responsible for identifying and prioritizing trends and developments within the United States and global innovation communities that will have NS/EP implications so that the relevant stakeholders may take steps to address anticipated dependencies, underinvestment or insufficient innovation in key areas, or to mitigate specific vulnerabilities and threats. The Senior Advisor will also initiate and oversee the development of national and international standards to help those responsible for NS/EP missions (NS/EP entities) assess the trustworthiness of ICT products, in coordination with the relevant D/As (interagency) possessing standards authorities, especially the National Institute of Standards and Technology, and relevant industry stakeholders.

Key Recommendations: U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem (*Section 4.2-4.2.6*)

To assist in carrying out the critical functions ascribed to the Senior Advisor, the NSTAC further recommends that the President direct the Senior Advisor to create a strategy to address how the Nation can increase the resiliency of critical NS/EP ICT, prioritize and coordinate action, and

streamline and accelerate innovation in the United States for NS/EP-critical technologies. A central objective of the strategy will be to implement policies that promote vibrant, diverse, and trusted supply chains for NS/EP-critical ICT and to advance competition to that end.

The following bullets summarize the key goals and sub-goals recommended for inclusion in the strategy:

- Define the means for government and industry stakeholders to work together in closer coordination to address the shared priority of ICT resilience. This will likely require an examination of legal barriers to coordination.

- Foster closer coordination among identified government stakeholders and elevate the mission within D/As of enabling resiliency and fostering innovation.

- Create the right conditions for strong domestic investment for manufacturers and innovators of NS/EP-critical technology.

- Survey the technology needs of NS/EP entities to identify where they could face diminished choices, dependencies, or insufficient innovation in ICT.

- Present a more strategic and cohesive U.S. position within international standards-setting processes and bodies by facilitating coordination among D/As and industry, identifying shared priorities and encouraging and incentivizing U.S. companies to participate more robustly.

- Look for creative ways for private firms and individuals to enable and support national security as a driver of their business decisions, including leveraging the Ecosystem Pillar activities contained in the *NSTAC Report to the President on a Cybersecurity Moonshot*.

- Define a shared national end state for all stakeholders. Describe actions toward that end state of key stakeholder groups including government D/As, technology creators and providers, critical infrastructure owners and operators, and the academic community and recommend ways government policies and programs can encourage these actions.

In addition to recommending the above, this report:

- Reiterates an *NSTAC Report to the President on a Cybersecurity Moonshot* recommendation that the President declare a national strategic intent and empower whole-of-nation resources to pursue a more fundamentally safe internet environment for critical services.

- Recommends leveraging the outcome of the Prague Fifth Generation (5G) Security Conference and ensuring that the proposals emanating from that conference remain at the forefront of international dialogue. As an outcome of the Prague conference, 32 participating nations noted the interdependence in the global ICT market landscape and the lack of a supply chain assurance process and described various procurement best practices and the importance of utilizing them.

- Supports the MITRE recommendation to create a National Supply Chain Intelligence Center but describes that this should serve the critical sectors and emergency preparedness communities, as well as the Department of Defense and the Intelligence Community.[2]

- Makes recommendations for improving cross-sector engagement, including describing the role that existing bodies such as the NSTAC and others can play moving forward.

- Describes the need to augment international dialogue and engagement on ICT security and resiliency.

- Recommends that the Office of Management and Budget create a budget function for strategic innovation and resiliency.

[2] MITRE, *Deliver Uncompromised*, https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf.

1.0 INTRODUCTION

The national security and emergency preparedness (NS/EP) missions of the United States increasingly depend on a broad and growing array of information and communications technology (ICT). The convergence of ICT and operational technology is occurring rapidly within the critical infrastructure sectors that underpin modern society. The Nation is reliant on ICT infrastructure for the functioning of society, including government and critical functions such as banking, utilities, healthcare, and transportation.[3] The pervasiveness and interconnected nature of ICT and the complexity of global ICT supply chains provides an increasingly broad set of vulnerabilities that malicious actors and adversaries know they can exploit. Whether adversaries' motivations are to quietly subvert critical systems in order to erode U.S. wealth and power over time, to disrupt or destroy these systems on a widespread basis at a time of their choosing, or both, the risk cannot be overstated.

> "We have created the infrastructure that creates all these dependencies that makes it feasible for an adversary to have this level of control."[4]
> *Dr. Thomas Donahue, former Senior Director for Cybersecurity National Security Council (NSC)*

The ICT that supports NS/EP missions must be available, reliable, and trustworthy. Concern over supply chain security and resiliency for NS/EP-critical technologies stems from the decreasing diversity of trusted companies that produce certain ICT, for example, certain fifth generation (5G) components. Diversity means that users of ICT can always find trusted ICT products made with trusted components and that there are trusted services available to implement and maintain the products. If trusted producers of certain ICT exit the market or are acquired, the United States could be forced to rely on technology providers that are subject to influence or control by adversarial foreign nations where government financial and managerial involvement in company decisions is common, there are inadequate legal and procedural safeguards to protect customers, and there is little transparent oversight of companies. A longer-term concern is that NS/EP-critical technologies may not be developed or produced in the United States at all, but instead in foreign countries, some of which may take an adversarial stance toward the United States and leverage that dependence for a strategic advantage during a conflict.

Threats to ICT supply chain security and resiliency exist in part due to the diminishing number of companies producing those technologies and components. Concern about the availability, reliability, and trustworthiness of ICT stems from U.S. experience thus far with several technologies that are already critical to NS/EP or will have major applications for NS/EP in the future. These include 5G wireless cellular technology, semiconductors, artificial intelligence and machine learning (AI/ML), and quantum computing. Many nations share the belief that these technologies are critical to their present and future national and economic security. The current global experience with 5G foretells a future in which the digitization of NS/EP functions provides a potential vector for adversarial compromise and disruption or destruction of this related infrastructure and supporting services. This report provides an in-depth examination of the security and resiliency concerns raised in connection with the deployment of 5G networks

[3] Department of Homeland Security, "National Critical Functions Set," https://www.dhs.gov/cisa/national-critical-functions-set.

[4] Thomas Donahue, "The Asymmetric Era as a Driving Need for a New Security and Economic Strategy." (Panel Discussion at the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019).

and informs how government and industry can better understand and advance resiliency for future NS/EP-critical ICT.[5]

Chinese Actions, U.S. Response

The Chinese government is pursuing a comprehensive strategy ("Made in China 2025") to ensure that China dominates global high-tech manufacturing.[6] The Chinese government desires for Huawei to become the top provider for components of global 5G infrastructure. This could significantly diminish choices in global telecommunication supply chains and create broad dependencies on Chinese technology. In pursuit of this strategy, China utilizes tactics such as economic espionage, forced technology transfer and unsupervised source code review to gain access to foreign technologies and duplicate them, thus allowing them to compete in the marketplace without investing in research and development (R&D). It further uses such tactics as subsidizing national champions; inundating the United States and other markets with significantly less expensive products from foreign government-subsidized national champion; using legitimate investment vehicles (e.g., venture, private equity, sovereign wealth funds, and acquisitions) to gain access to intellectual property (IP); and enrollment in key U.S. universities to gain access to IP of the most promising emerging technologies.[7]

The U.S. Government has expressed concern to U.S. businesses and allied foreign nations about security risks associated with telecommunications components integrated into critical/privileged locations within a carrier's network. Congress passed a law that prohibits federal agencies from purchasing certain Chinese telecommunications technology equipment and services, limits private entities that receive U.S. federal funding from utilizing certain covered equipment,[8] and asks its allies to institute similar prohibitions.

Supplier diversity is also being challenged by China in areas beyond 5G network infrastructure and equipment. China's desire to decrease its national reliance on U.S.-made semiconductors holds significant implications for U.S. ICT security and resiliency and is examined in greater detail in Appendix B.

1.1 Scoping and Charge

In August 2018, the White House tasked the President's National Security Telecommunications Advisory Committee (NSTAC) to examine technology capabilities that are critical to NS/EP functions in the evolving ICT ecosystem. The White House tasked the NSTAC to study the issue in two phases. The first phase required the NSTAC to examine current technology capabilities across the ICT ecosystem that are most critical to the Government's NS/EP functions in the next five to ten years. In a letter to the President dated April 2, 2019, the NSTAC completed the first phase and identified three representative technologies highly critical to the U.S. NS/EP mission: 5G wireless technology; quantum computing; and AI/ML. The second phase of the tasking required the NSTAC to make recommendations for enhancing resiliency and fostering innovation, and this report does so with consideration of the technologies identified in phase one.

[5] See Appendix A: 5G Case Study.

[6] James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, last updated May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

[7] Office of the United States Trade Representative, Executive Office of the President. "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974." March 22, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[8] 115th Congress (Cong.), 2nd Session (Sess.), House of Representatives (HR) 5515, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," Section 889, https://www.congress.gov/bill/115th-congress/house-bill/5515.

2.0 THE DESIRED END STATE

NS/EP entities must have vibrant and diverse choices of trusted technologies and technology providers. U.S. policy must endeavor to create this ecosystem of vendor diversity for NS/EP-critical ICT. The U.S. Government must coordinate more closely with industry to be able to identify trends that threaten the security and resiliency of the supply chains for ICT technology that enable and support (or will enable and support) NS/EP functions. The goal is not for the U.S. Government to pick winners and losers, but rather to foster the conditions that sustain key manufacturing capabilities and capacity in face of unfair foreign support and to keep the United States on the forefront of innovation, to the greatest extent possible, in strategically important areas of technology. The U.S. Government must help industries that are, or will be, critical to the success of U.S. NS/EP, and to ensure policies that are harmful to them are minimized.

Desired End State

- Those responsible for NS/EP missions must have vibrant and diverse choices of trusted technologies and technology providers.
- The U.S. Government must coordinate closely with industry to identify trends that threaten the security and resiliency of the supply chains for ICT technology that enable and support (or will enable and support) NS/EP functions.
- The U.S. Government must foster the conditions that sustain key manufacturing capabilities and capacity in the face of unfair foreign support and to keep the United States on the forefront of innovation, to the greatest extent possible, in strategically important areas of technology.
- The U.S. Government must help industries that are, or will be, critical to U.S. NS/EP to be successful, and to ensure policies that are harmful to them are minimized.

The United States currently lacks a methodology for identifying, in advance, the reduction of manufacturing capacity as well as faltering innovation that could have short-term and long-term impacts on NS/EP missions. The Government must have a means to constantly and strategically survey the technology needs of federal and emergency preparedness agencies and critical sectors. This must be compared to trends and developments within R&D and innovation communities within government, the private sector, and academia. The Government must seek to foster the conditions in which the companies that develop and produce current and future technology upon which NS/EP depends can thrive. The goal is not to shield U.S. companies from competition, as competition is a major driver of excellence in innovation and a strategic differentiator for the United States. Additionally, competition creates a vibrant global ICT marketplace and ensures that NS/EP entities have ample choices.

The U.S. Government must also seek to level the global playing field when government support and subsidies create unfair advantages, or economic artificialities, for foreign competitors.[9]

To achieve this, the Government must:

- Analyze the ICT market and submarkets for the health of key technology creators and providers, as well as the impact of predatory behaviors, both from a national security and an economic standpoint, by adversarial nations.

[9] Department of Homeland Security Cybersecurity and Infrastructure Security Agency Director Christopher Krebs. (Comments During the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019).

- Adopt policies that create the conditions that encourage new companies to enter key technology sectors and markets or for companies in existing markets to remain.

- Improve existing mechanisms for collaboration on national strategic priorities with the manufacturing and innovation communities and the critical sectors.

- Expand initiatives that encourage American companies to innovate.

- Encourage innovation community stakeholders to build strong security into products and to factor national security imperatives in their decision-making.

- Collaborate more closely with business executives within the critical sectors to ensure that they know the true risk of relying on ICT that could be compromised and under the influence of adversarial foreign nations.

The Innovation Community

The innovation community, which is described more fully in Section 4.2.1, *Identify Stakeholders*, generally encompasses individuals and organizations from the private sector and academia that are involved in developing new technologies and bringing them to market. Organizations from the private sector that are part of the innovation community are referred to in this report as Technology Creators and Providers. The innovation community also encompasses government stakeholders, since the U.S. Government is a major user/consumer of these technologies and has multiple agencies and programs dedicated to supporting U.S. businesses, R&D, and technology development**.**

2.1 Factors Preventing the Desired End State

In the research phase of this report, the NSTAC examined the development and deployment of 5G in the United States as a case study (see Appendix A). That analysis, in addition to the briefings provided to the NSTAC, allowed the NSTAC to draw conclusions about how some concerning dependencies, market limitations, and supply chain risks began. The core conclusions drawn, and those that NSTAC will apply to current and future NS/EP-critical ICT, include the following:

- The U.S. Government is not currently organized effectively to foster the desired end state, an ecosystem of vendor diversity for NS/EP-critical ICT.

- National security and economic security decision making are not sufficiently coordinated.

- There is no office or position within the Government that is accountable for coordinating between the national security and economic agencies/components and with non-government stakeholders such as industry and academia.

- There have not been strong enough relationships built between appropriate U.S. Government agencies, including national security agencies, and the manufacturing and innovation communities.

- The U.S. Government has not adequately analyzed the health of the ICT marketplace or the sale of some ICT companies to foreign-based companies. In some segments of the ICT market, notably the radio access network (RAN), there has been a trend toward fewer choices of products for users. Future oversight is critical to mitigate such trends.

- Technology creators and providers should improve how they are organized to address the mutual challenge of strengthening ICT resiliency.

- Manufacturing capacity within the U.S. for certain technologies has diminished and government and industry in the United States have not invested enough in R&D in basic science or for technologies without a well-defined path to market.

- The U.S. Government has not maintained adequate awareness of the manufacturing and innovation communities based in allied countries, as some of the needs of U.S. NS/EP missions can be met (and probably will need to be met) by trusted companies based in foreign allied nations.

- Finally, the U.S. Government, industry, and academia have not taken strong enough action in response to the theft of U.S. IP by foreign countries such as China.

5G Case Study

5G is the next generation of wireless communications technology building upon and succeeding fourth generation/long term evolution (4G/LTE). 5G networks enable significantly faster speeds, lower latency, and greater component functionality. Moreover, 5G will enable a range of applications driving significant technological advances adding $500 million to U.S. gross domestic product and three million jobs.[10] As a result, the next age of digital transformation depends on the success of the 5G build out in the United States.

As discussed in the NSTAC *Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*, there are concerns about the growing presence of Chinese telecommunications equipment manufacturers, particularly in networks outside of the United States, and the long-term implications for 5G and the broader communications and internet technology supply chain. This concern is particularly acute in the RAN portion of the network where there are a limited number of RAN equipment suppliers.

A primary root of this concern is the growing presence of subsidized competition from China. If Chinese manufacturers continue to gain market share, there is growing concern about the long-term viability of the existing supply chain for 5G and successor technologies. The consolidation of vendors has decreased vendor diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and R&D all work to discourage new communications vendors from competing with established players. However, there are opportunities to correct this in the future.

As networks have evolved toward software-defined networking (SDN) and network function virtualization, these developments may provide an option to address supply chain concerns by driving the industry toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace.

However, the United States needs to put in place the right policy framework to support these developments. In the short term, government can support more innovation in the ecosystem by promoting policies that promote vendor diversity and competition in the supply chain, encourage the use of open standards in the RAN and enhanced interoperability, such as the standards under development at the Open Radio Access Network (O-RAN) alliance, foster participation in standards setting bodies, and develop a more cohesive government-wide 5G strategy. In the long term, the government should look at creating economic incentives for investment in these emerging technologies, incentivizing industry action and adoption of U.S.-based technologies across the private and public sectors, strengthening the countries expertise and innovation, and protecting IP.

2.2 What the United States Government Is Getting Right

Policymakers have recently begun to take bold actions to address some of these shortcomings.

Legislative Branch Actions

- In August 2018, Congress passed the *Foreign Investment Risk Review Modernization Act of 2018* (FIRRMA), which expands Committee on Foreign Investment in the United States

[10] Accenture, **"**New Research from Accenture Strategy highlights Economic and Societal Impact of Investing in 5G Infrastructure**,"** https://newsroom.accenture.com/news/new-research-from-accenture-strategy-highlights-economic-and-societal-impact-of-investing-in-5g-infrastructure.htm.

jurisdiction to review non-controlling foreign interests in critical infrastructure, critical technologies, or sensitive personal data.[11]

- In December 2018, Congress passed the *SECURE Technology Act*, which, among other things, raised security to a co-equal factor in federal procurements (along with cost and timeliness) for the first time. The act also established the Federal Acquisition Supply Chain Security Council which is broadly charged with developing policies and requirements for federal supply chain security. This created a central federal-wide focal point for procurement security policies and processes for the first time. The council will oversee the development of National Institute of Standards and Technology (NIST) guidelines on supply chain risk management, create information sharing protocols between federal and non-federal entities, establish a lead agency to oversee the information sharing process, and investigate solutions that can be leveraged in the federal contracting process.[12]

Executive Branch Actions

- In July 2018, the Department of Homeland Security (DHS) ICT Supply Chain Risk Management Task Force brought the public and private sectors together to address key strategic challenges to identifying and managing risk associated with the global ICT supply chain.[13] Section 5 of Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, requires the Secretary of Homeland Security to produce a written assessment identifying the "entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the United States' national security."[14]

- In 2018 the Department of Defense (DOD) stood up the Protecting Critical Technologies Task Force as an organizing initiative to address defense industrial base supply chain risk and resilience issues across the Department, and in partnership with industry.

---

[11] Thilo Hanemann and Daniel Rosen, "China in the ICT Ecosystem," (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, March 12, 2019).

[12] 115th Congress (Cong.), 2nd Session (Sess.), House of Representatives (HR) 7327, "Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act," https://www.congress.gov/bill/115th-congress/house-bill/7327/text.

[13] Department of Homeland Security, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

[14] White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Promising Models for Collaboration at the DOD and the Intelligence Community (IC)

Public-private collaboration initiatives pioneered by DOD and the IC provide models to be considered by the Senior Advisor for extensibility to the broader community, with some appropriate adjustments.

The Defense Advanced Research Projects Agency's Electronics Resurgence Initiative program facilitates partnerships between government, industry, and academia and meets national security objectives by fostering advances in materials, semiconductor circuit design, and system architectures that address the physical challenges imposed by Moore's Law and threats from Chinese industry.[15] The IC Advanced Research Projects Agency also provides a model.

In-Q-Tel (IQT) was established in 1999 to ensure that the U.S. intelligence agencies had access to innovative technologies from the startup community to help protect and preserve U.S. security.[16] IQT surveys the technology landscape and identifies advantageous technologies to support, particularly in circumstances where a traditional R&D contract would not work. IQT has a history of seeding companies that are sensitive to U.S. national security interests throughout their existence.

More recently, the DOD has focused on innovation and rapid acquisition and has created structures to achieve this. For example, the Defense Innovation Unit as well as initiatives within the services such as Army Futures Command and the Air Force's AFWERX are having success in nurturing relevant startups and are excellent hubs for collaboration, having delivered new capabilities to their respective Services on timelines measured in months rather than years. However, these bodies have difficulty helping startups mature to a point of winning contracts that generate revenue. Other transaction authority (OTA) has helped bridge this gap, but processes and rules for OTAs are not well-defined and inconsistently applied, potentially creating more problems than they solve.

Tools and methods utilized by the DOD can be helpful models for work on broader innovation efforts, but their suitability for application to the general economy should be carefully considered. More adjustments may need to be made to promote flexibility and encourage private actors to take on risks and work with the Government. Programs like these should emphasize commercialization of the technology over Government control of IP to encourage more startup collaboration with the Government.

[15] Defense Advanced Research Projects Agency (DARPA), "DARPA Electronics Resurgence Initiative," https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.

[16] In-Q-Tel, "Our History," https://www.iqt.org/our-history/.

- In February 2019, the White House prioritized the "Industries of the Future" which identifies AI, advanced manufacturing, Quantum Information Science (QIS), and 5G as the emerging technologies fundamental to America's future.[17] The strategic focus on these technologies has manifested in several new programs and initiatives.

- EO 13873, implementation of which is being led by the Department of Commerce (DOC), seeks to limit the acquisition and use in the United States of ICT or services that are "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries."[18] The EO has rightfully highlighted the seriousness of the threat posed by untrusted ICT (or ICT that could be controlled by foreign adversaries) and calls for measures to ensure, to the greatest extent possible, that such ICT is not permitted to be incorporated into networks that support NS/EP missions in the United States.[19] The NSTAC views the EO and the prohibition of specific products or manufacturers as one potential part of what should be an overarching strategy to address the Nation's strategic ICT resiliency and innovation challenges. Excluding products that are found to be untrustworthy is one of several policy changes that could be considered to address these challenges but is not the only tool. Restrictions like those called for in the EO

What is "Trusted?"

Trusted technology is technology that is designed, produced, tested, delivered, and serviced following a predetermined set of actions and protocols (see section entitled, "Standards for Evaluating Risk of ICT") in accordance with specifications set by customers and not under the influence by any foreign government. It is defined by actions, not origin. "Foreign-made" does not mean inherently untrustworthy, just as "U.S.-made" or "allied-made" does not mean inherently trustworthy.

NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, contains a useful discussion of trust and trustworthiness. It defines trustworthiness as: "An attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities." (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf)

DOD has had success in establishing processes and policies for minimizing third party cybersecurity risk and procuring only trusted technologies, for example, through the DOD Information Network (DODIN) Capabilities and Approved Products List (APL) as well as for ensuring, for example through the Trusted Foundry program, that there are manufacturers for those technologies. The DOD APL involves a rigorous testing and certification program products must pass before they can connect to the DODIN. The Trusted Foundry is a DOD program that aims to secure the manufacturing infrastructure for information technology vendors providing hardware to the military. In 2016, the Defense Science Board delivered a report assessing the organization, missions, and authorities that encompass the use of microelectronics and components in DOD weapons systems. Notably, the task force recommended that the Department develop a long-term strategy for access to state-of-the-art commercial foundry capabilities that does not rely exclusively on trust and continue R&D investments into new tools to better defend against cyber attacks targeting the supply chain.

This report discusses the need for standards to help NS/EP entities assess the trustworthiness of ICT products in the section entitled, "Standards for Evaluating Risk of ICT."

[17] White House, "America Will Dominate the Industries of the Future," https://www.whitehouse.gov/briefings-statements/america-will-dominate-industries-future/.

[18] White House, "Executive Order on Securing Information Communications Technology and Services Supply Chain," https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[19] *Ibid.*

can be part of a holistic National ICT Resiliency and Innovation Strategy as developed by the Senior Advisor to the President for ICT Resiliency.

- The U.S. Government has taken some positive steps on the innovation side of the problem. EO 13859, *Maintaining American Leadership in Artificial Intelligence* and the *National Quantum Initiative Act*, elevated these two technologies as national priorities. Both initiatives are discussed in greater detail later in this report.

3.0 THE CHALLENGE

The United States faces a twofold challenge regarding the security and resiliency of NS/EP-critical ICT. First, adversarial nations actively seek to displace U.S. and western manufacturers as the leading producers of NS/EP-critical ICT. Driving adversaries' behavior is the desire to overtake the United States as the world leader in innovation, particularly with respect to NS/EP-critical ICT. Second, there is significant concern that the quality and pace of innovation in the United States (especially as it concerns NS/EP technologies) could one day be surpassed by foreign adversaries. Adversarial nations have begun to invest heavily in the development of such technologies, and they employ both legal and illegal means to misappropriate U.S. IP relating to strategic technologies for their own security and economic benefit. Legal means include acquiring U.S. telecommunications and networking equipment providers or making large investments in shares of U.S. technology and internet companies.[20] Illegal means include computer intrusion campaigns carried out by well-organized hacking groups, such as Advanced Persistent Threat 10, that target IP and confidential business information and have known ties to Chinese government organizations.

China's desire to displace U.S. and western manufacturers as the leading producers of NS/EP-critical ICT is a major factor in driving this behavior. The U.S.-based manufacturing capacity for certain technologies has been eroded in part because it is almost always cheaper to produce certain technologies outside of the United States. However, the erosion is in large part attributable to the deliberate and coordinated efforts of certain foreign nations, especially China, to promote, support, and subsidize their own manufacturers of strategically important technologies. Their goal in doing so is to ensure such manufacturers can increase their penetration of global markets and, in some cases, reduce or eliminate their own dependence on U.S. and western products thereby enhancing their national security. Furthermore, such manufacturers are subject to the laws of foreign nations where government financial and managerial involvement in company decisions is common, there are inadequate legal and procedural safeguards to protect customers, and there is little transparent oversight of companies. The exit or acquisition of trusted U.S. and allied-based manufacturers has resulted in fewer choices of trusted products and providers to fulfill those missions. China's policies have played a significant role in the decline of U.S. hardware manufacturers. In the case of 5G, explored more fully in Appendix A, U.S.-based companies exited the RAN market because of an unlevel playing field created by China's subsidization of Huawei. China's support for Huawei allows it to deliver networking products at far below fair market value. Today, Huawei has nearly 38 percent of the global RAN market.

[20] Thilo Hanemann and Daniel Rosen, "China in the ICT Ecosystem." (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, March 12, 2019).

EO 13873, *Securing Information Communications Technology and Services Supply Chain*

EO 13873, *Securing Information Communications Technology and Services Supply Chain*, found that "The unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." Many companies in China often either are directly owned in whole or part by the government. A well-known requirement of businesses that operate in China is that they must include representatives of China's Central Party on their boards and/or executive leadership.

The second challenge the United States faces regarding NS/EP ICT security and resiliency is that adversarial nations may one day surpass the United States in their ability to invent advanced technologies that might be used against the Nation, or upon which United States may become reliant for NS/EP missions. Although the United States remains among the most attractive places in the world for innovators, the U.S. Government has severely underinvested in R&D in raw science for the past ten years. Where R&D has received Government support, there has not been overarching direction toward national strategic goals.[21] The current strategies being employed by China to advance its development of AI/ML, semiconductor technology, and quantum computing technologies bring the dichotomy with the United States sharply into focus. China is investing significant resources into building up its internal R&D infrastructure in part to advance its efforts in these areas.[22]

In addition to investing in its own R&D capabilities, China is also utilizing legal investment mechanisms within the United States and other markets (e.g., venture, private equity, sovereign wealth funds, and acquisitions) as well as enrollment in U.S. universities to gain access to the IP associated with the most promising and strategic emerging U.S. technologies. China also uses tactics such as forced technology transfer or unsupervised source code review provisions for access to desired IP. Finally, it is widely known that hacking groups tied to the Chinese government use technical means to steal desired IP and transfer it to Chinese companies and the government.[23]

[21] Thomas Donahue, "The Asymmetric Era as a Driving Need for a New Security and Economic Strategy." (Panel Discussion at the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019).

[22] Elsa Kania, "China's Quantum Future," https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

[23] Federal Bureau of Investigation, "Chinese Hackers Indicted," https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

AI/ML and Quantum Case Study

With respect to AI/ML and quantum computing, the United States has recognized the problems and responded with specific programs and decisions, with rare examples of expedient cooperation between the White House and Congress. The U.S. Government has already acted, recognizing the need to ensure the United States remains at the forefront of innovation with respect to these two important technologies. On February 11, 2019, President Trump issued EO 13859, *Maintaining American Leadership in Artificial Intelligence*. The issuance of this EO was an important step towards ensuring that AI development is elevated as a major national priority and addressing the challenge of keeping pace with China and other countries. The Fiscal 2020 R&D Budget Priorities document issued by the White House in July 2018 was the first to ever prioritize AI on a national basis. While continued cooperation with like-minded nations will be essential, the White House's strategic emphasis on "dominating" and "winning" these industries of the future appropriately recognize that adversaries view these technologies as opportunities to gain strategic leverage against the United States.[24]

On quantum computing, the United States enacted the *National Quantum Initiative Act* (Public Law 115-368) in December 2018, which signaled both Congressional and White House concern over the threat that the United States may fall behind in quantum computing development. The law, among other things, establishes a 10-year plan to accelerate the development of QIS with White House-led strategic oversight, and funds U.S. Government efforts to lead collaborative R&D efforts aligned to QIS and its technology applications. It also provides a useful model for the appropriate role of the U.S. Government in fostering open innovation across the public, private, and academic sectors. The White House has also created a National Quantum Coordination Office to harmonize D/A QIS activities and foster a broader QIS industrial ecosystem.

Congress and the White House both are to be commended for recognizing the need to stay at the forefront of these fields and to provide both the structure and funding within the government to support U.S. public and private efforts. These are excellent examples of not waiting until the problem becomes a crisis. However, these efforts need to be coordinated across government and structures need to be in place to identify and respond to future security and resiliency issues facing NS/EP-critical ICT.

Looking to the future, there must be a single place in government tasked with continuously surveying the innovation community and beyond to determine what technologies today, five years and ten years in the future deserve the same level of prioritization because of their current or future applications for NS/EP. The U.S. Government must do everything within its authorities, and may require some additional authorities, to ensure that trusted manufacturers remain in key markets and to create the conditions that foster American innovation in key areas. The Nation must be realistic about the fact that it is impossible to manufacture all ICT in the United States. However, the Government must carefully identify NS/EP-critical ICT and ensure that the United States remains at the forefront of its development and deployment. The U.S. Government must work resolutely with private sector partners and foreign allies to this end.

[24] Executive Office of the President, "Memorandum for the Heads of Executive Departments and Agencies-FY 2020 Administration Research and Development Budget Priorities," https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf.

4.0 RECOMMENDATIONS

The NSTAC believes that U.S. Government efforts should encourage the availability, evolution, and use of trusted technologies, particularly for those sectors/companies which directly or indirectly support NS/EP missions. There must be a stronger national commitment to creating and preserving vibrant, diverse, and trusted supply chains for NS/EP technology, and stronger central coordination of all U.S. Government efforts toward that end. The United States requires a holistic national strategy and a dedicated White House position to coordinate the development and implementation of that strategy across U.S. D/As (especially the national security community), the critical infrastructure provider community, and the innovation community.

Therefore, the NSTAC recommends that the President:

- Create, by issuance of an EO, the position of a new Senior Advisor to the President for ICT Resiliency.

- Empower the Senior Advisor to lead the interagency development and implementation of a national policy and Strategy on advancing ICT resiliency and fostering innovation in close coordination with the National Security Advisor, the Director of the National Economic Council (NEC), the Director of Office of Science and Technology Policy (OSTP), the heads of the relevant D/As, and relevant private sector stakeholders.

The central goal of the Strategy will be to ensure vibrant, diverse, and trusted supply chains for NS/EP-critical ICT, and to promote competition to that end. The NSTAC recommends many goals and sub-goals be considered for inclusion in the Strategy which are described in Section 4.2, *U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*.

4.1 Senior Advisor to the President for ICT Resiliency

Recognizing the complexity of challenges facing the Nation with respect to ICT resiliency and innovation, the NSTAC believes the United States requires a whole-of-nation approach and dedicated senior White House position. These complex challenges include the fact that NS/EP resiliency touches many diverse public and private stakeholder groups, is multi-disciplinary in nature (e.g., involves technology, economic, geopolitical and governance issues), and that foreign adversaries are carefully coordinating their own efforts to dominate in this space. Recognizing these factors, the United States needs a central focal point that can organize the Government and the Nation more broadly as it takes on these challenges. The Senior Advisor will provide cohesion and direction to national efforts relating to strategic ICT resiliency and innovation. The Senior Advisor will be responsible for setting national ICT resiliency and innovation goals and for creating, coordinating, and implementing government policies and activities in support of those goals. The Senior Advisor will lead the development and implementation of an ICT Resiliency and Innovation Strategy to more effectively align the national security, critical infrastructure provider, and innovation communities. It will be the responsibility of the Senior Advisor to coordinate among national security agencies and to foster a focused, regularized engagement with the broader stakeholder community. The Senior Advisor will constantly and strategically survey the technology needs of U.S. defense and intelligence

agencies, federal and emergency preparedness agencies, and critical sectors to compare those needs to trends and developments within U.S. and global innovation communities. This will ensure that steps can be taken in coordination with the national security, critical infrastructure provider and innovation communities to address anticipated dependencies or insufficient innovation, or to mitigate significant threats to national security. Innovation is not something that exists in a single place; it often bubbles up in unexpected places and at unexpected times throughout the innovation community and is not simple to track. The Senior Advisor should look to existing models for effectively and continuously surveying emerging technology.[25]

The President must clearly articulate the mission, goals, and authorities of the Senior Advisor. The NSTAC recommends that the Senior Advisor be given the ability/authority to:

- Coordinate the strategy and policy generating elements of the White House relating to ICT resiliency.

- Advance policies to ensure the United States is taking appropriate steps to achieve national ICT innovation and resiliency goals and utilizing all available government levers to elicit the desired actions from the stakeholder groups, as and described in this report and ultimately delineated in the Strategy.

- Advance policies or take certain actions through the appropriate federal agencies in the interest of U.S. national security and/or NS/EP continuity of operations in response to identified threats, gaps, or problematic trends that may impact the actions of both U.S. Government and non-government stakeholders domestically and internationally.

- Convene and/or task all the relevant Federal Government stakeholders, particularly those whose missions deal with national security and innovation, to ensure they are working together, have adequately prioritized national security and innovation and other related missions, and are implementing the policies set forth by the President and Senior Advisor.

- Convene and coordinate with non-government partners, especially leaders from the manufacturing and innovation communities, the critical sectors, and academia, utilizing existing processes already established by federal agencies and federal advisory committees.

- Survey the technology needs of NS/EP entities to identify where they could face diminished choices, dependencies on untrusted products or manufacturers, or insufficient innovation in ICT. The Senior Advisor should also be mindful of other dependencies (e.g., rare earth minerals, shipping limitations) that can also adversely impact NS/EP functions.

- Identify NS/EP-critical ICT across the vast global digital economy, as much as ten years in advance of it having an impact on U.S. resiliency and/or U.S. national security, by working in coordination with the innovation community and relevant federal D/As. Following identification, articulate the impact of such technologies on national resiliency and/or security and create and oversee the implementation of the necessary approaches to address

[25] Department of Defense, "Summary of the 2018 DOD Artificial Intelligence Strategy-Harnessing AI to Advance our Security and Prosperity," https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

anticipated dependencies or insufficient innovation, or to mitigate specific threats. The Senior Advisor must take care not to exclude categories of ICT from consideration merely because their importance to NS/EP is not yet predictable or clear.

The Senior Advisor should have a seat on the NSC and NEC and should be empowered to lead interagency development, coordination, and implementation of policies through the NEC and NSC's respective policymaking processes.

The new leadership structure described in this report is the natural evolution of the Administration's demonstrated desire to be better coordinated and equipped to manage issues relating to ICT resiliency and innovation. The NSTAC recommends that the President eventually combine other existing White House efforts on AI/ML and quantum (to the extent feasible under the authorities under the *National Quantum Initiative Act*) under the guidance of the Senior Advisor. The President should evaluate how existing bodies created under the auspices of the AI/ML EO and the quantum legislation should interact with the Senior Advisor and should clearly delineate responsibilities and authorities.

Federal Government Stakeholders

The Senior Advisor will seek to implement the Strategy mainly through the authorities and operations of existing federal agencies. The federal agencies and components with whom the Senior Advisor will collaborate and who will play a role in developing and executing the Strategy include but are not limited to: the Office of Management and Budget (OMB), OSTP, the Office of American Innovation, the NSC, NEC, the U.S. Trade Representative, DOC (including the National Telecommunications and Information Administration, NIST with regard to standards, the International Trade Administration, and the Bureau of Industry and Security (BIS), the National Science Foundation (NSF), DHS (Cybersecurity and Infrastructure Security Agency (CISA), the IC (including the Director of National Intelligence and others, as appropriate), DOD, the Department of Justice, the Department of Energy (DOE), the Department of State in regard to international engagement, and the Department of Education.

4.2 U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem

The NSTAC recommends that the Senior Advisor create and implement, in coordination with other relevant stakeholders, a national policy and U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem. This Strategy must directly address how the United States can accelerate the development of critical NS/EP technologies and ensure a vibrant, diverse, and trusted supply chain for NS/EP-critical ICT. The Strategy should attempt to promote competition by lowering barriers to entry, support the use of open standards, encourage R&D in critical technologies, and incentivize U.S. companies to lead the world in the development and deployment of cutting-edge technologies.

The Strategy should strive to be predictable and enduring, to foster reliance and trust on the part of the private sector actors who are choosing where to invest and innovate. If companies' efforts toward both compliance and risk management are subject to uncertainty and shifting government priorities, they may not view the U.S. Government as a trusted partner.

The Strategy should encompass (but need not be limited to) six sub-goals:

1. **Identify the stakeholders** critical to achieving the resiliency and innovation goals outlined in the Strategy. Recommend specific mechanisms by which the U.S. Government can help

foster idea and information exchange, as well as policy coordination and collaboration, amongst key stakeholders. Much of the change that needs to happen involves private sector action, reinforced where appropriate by Government.

2. **Create a multi-stakeholder process** to solicit recommendations from the identified stakeholders to advance the resiliency of NS/EP-critical ICT.

3. **Identify gaps in policy, budget, and authorities** that hamper the achievement of the Strategy's goals and develop and implement a plan for closing those gaps, including granting new authorities where necessary.

4. **Identify and leverage the U.S.' natural strategic advantages** in order to seek to leverage, to the maximum extent, the aspects of the U.S. society and economy that confer advantages upon the Nation as the United States seeks to maintain its global preeminence in innovation.

5. **Foster stronger cooperation amongst like-minded nations** to ensure vibrant, diverse, and trusted global supply chains for ICT products. Given the interconnectedness of networks, the challenge of ICT security and resiliency is an international issue, and it is impossible to address the roots or the impacts of this problem from a U.S.-only perspective. The United States must consider what international fora and bodies facilitate international dialogue and engagement on ICT security and resiliency and seek to augment this dialogue and engagement.

6. **Verify that the U.S. Government utilizes its authorities and capabilities** to ensure that it is properly aligned and resourced to support the achievement of the overarching goal and sub-goals of the Strategy. Ensure that those authorities and capabilities are well-coordinated, and objectives are achieved efficiently.

The sub-goals are each described in greater detail in the sub-sections below.

4.2.1 Identify Stakeholders

One of the core responsibilities of the Senior Advisor will be to bring together a community of interest (COI) around advancing resiliency and fostering innovation. The participation of stakeholders from across the COI is critical to the achievement of the resiliency and innovation goals outlined in the Strategy. The COI can be thought of as drawing from and leveraging both the national security community, the innovation community and the critical infrastructure provider community (e.g., the end users of ICT). The COI encompass a wide range of individuals from the key stakeholder groups including the U.S. Government, the private sector, academia, and non-government organizations/standards bodies. The national security community generally encompasses people in the U.S. Government and within U.S. defense and civilian contractors who support NS/EP, in this case, individuals who understand the international and national security landscape and who understand how ICT supports NS/EP missions. For a list of government stakeholders, see Section 4.1, *Senior Advisor to the President for ICT Resiliency*. The innovation community generally encompasses individuals and organizations from the private sector and academia that are involved in developing new technologies and bringing them to market. The innovation community also encompasses government stakeholders, since the U.S.

Government is a major use and consumer of these technologies and has multiple agencies and programs dedicated to overseeing and supporting U.S. businesses, R&D, and technology and services development and delivery.

There is a priority need for closer relationships between those who are responsible for overseeing national security policy and functions, for example, those who understand how ICT underpins NS/EP missions, and those responsible for the development, manufacturing, and delivery of strategically important ICT. Some of the factors that may have prevented close relationships between these communities in the past includes the fact that the innovation community is fragmented, and the U.S. Government does not provide enough value to the innovation community. Hurdles to cooperation between these communities include overly-burdensome requirements on federal funding, the slow pace and often uncertain and inconsistent funding stream associated with government contracting opportunities, onerous constraints on IP created under government partnerships, and a lack of trust and liability uncertainty with respect to information sharing. If the Government, led by the Senior Advisor, is to have a more collaborative relationship with the innovation community, it will need to be more active in how it communicates its needs and articulates the mutual value in working together. Together, they will need to develop better ways to reward a balanced approach to innovation, security, and resiliency.

Stakeholders from the innovation community that have fruitful and regularized relationships with national security community are more likely to have cognizance of NS/EP implications of emerging technologies. They may better understand the non-monetary implications of pursuing certain technologies. They may be less likely to participate in or fall victim to the tactics employed by adversarial nations to pilfer their valuable IP. They may also implement more robust practices designed to counter IP theft, including more thoughtful consideration of certain funding sources, partners, employees, and more. The story of Bell Labs provides a notable model for public-private collaboration. Bell Labs had the resources, talent, and culture to produce some major technological advancements of the 20th century with significant commercial and national security benefits.[26]

4.2.2 Identify Desired Actions

The NSTAC has identified some desired actions by stakeholder groups that should be considered by the Senior Advisor in formulating the Strategy.

Government

The Government must have and exercise the necessary authorities to ensure that a diverse set of trusted manufacturers remain in key markets and help foster American innovation. Working with government personnel, industry representatives, and members of academia, the Government should:

[26] Quora, "Why Bell Labs was so Important to Innovation in the 20th Century," *Forbes*, July 19, 2017, July 3, 2019, https://www.forbes.com/sites/quora/2017/07/19/why-bell-labs-was-so-important-to-innovation-in-the-20th-century/#5e568db7015f.

- Elevate and embrace the objective/mission of enabling resiliency and fostering innovation within the U.S. economy.

- Articulate security imperatives to and collaborate with the non-government stakeholder groups to implement the Strategy.

- Foster R&D and the commercialization of critical technologies.

- Create more reliable and useable intelligence and better intelligence sharing mechanisms with stakeholders in the private and academic sectors. The Senior Advisor should examine the ways information is shared by D/As for whom providing such information sharing and awareness-building is a part of their core mission, for example, the Centers for Disease Control. The Senior Advisor could also examine international bodies known to be effective at information sharing such as the World Health Organization. The Senior Adviser should decide which stakeholder groups should be designated as customers of intelligence. This designation would allow certain stakeholders to receive information from the IC in an appropriate form and ask them to identify and prioritize their intelligence needs and provide feedback on intelligence use to the IC.

- Provide better assistance to U.S. companies to help them prevent IP theft by adversarial nations; help them improve response when IP theft occurs; and help them adopt best practices in counterintelligence, as well as other areas (especially the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation, and U.S. Secret Service).

- Move to outcomes-based regulation and eliminate requirements that generate workstreams and record-keeping without improving resiliency.

Technology Creators and Providers

Technology creators and providers should be incentivized to advance the resiliency and innovation goals outlined in the Strategy. This means that industry should be incentivized to: (1) increase interaction and collaboration with the Government; (2) provide information about emerging NS/EP technologies; (3) give more consideration to national security interests in their business decision making; (4) increase participation in standards setting; and (5) take more enthusiastic ownership of workforce challenges that may threaten or limit U.S. manufacturing or innovation capacity. The Strategy must also identify recommendations for how to achieve these desired actions and should consider both positive and negative incentives. There are several actions the U.S Government could take, many under the leadership of the Senior Advisor, to drive desired behavior by technology creators and manufacturers including:

- Create the right conditions for strong investment domestically and a level playing field globally, such as lowering taxes, promoting the construction of state-of-the-art facilities, and pursuing anti-dumping action in trade bodies. The Senior Advisor could also consider previous policies that have, to varying degrees, advantaged U.S. producers of goods needed by government agencies, including the "Buy American Act," which requires federal agencies

to purchase domestic end products and use domestic construction materials on contracts exceeding a low threshold.[27]

- Offer specific incentives (such as tax incentives) for companies to invest in R&D, particularly raw science, or to companies that prioritize or donate to science, technology, engineering, and math (STEM) workforce development efforts. Encourage private sector grants to academic institutions for research and training on critical/identified NS/EP technologies.

- Leverage the purchasing power of the Government and NS/EP community to provide incentives to deliver economically viable, security-enhanced products and services.

- Identify ways to help innovators and entrepreneurs of NS/EP relevant technologies overcome the gap innovators face in moving an idea from conception to market.

- Remove barriers/disincentives to partnering with the U.S. Government, such as restrictive contract covenants and overly burdensome contracting requirements (like those included in the Federal Acquisition Regulation and some Cooperative R&D Agreements) and move government acquisition policies away from the practice of Lowest Price Technically Acceptable for the procurement of ICT products and services.[28]

- Present a more cohesive and strategic U.S. position within standards-setting processes and bodies by facilitating coordination among D/As and industry and encouraging and incentivizing U.S. companies to participate more robustly.

- Work with stakeholders within the innovation community, so they are more aware of the economic benefits of building stronger security features into products and develop best practices and metrics to better incorporate security and resiliency as a best value consideration in contracting.

- Promote the use of interoperability, open interfaces, and modular design because of their business benefits and their ability to enable security and resiliency.

- Make it easier for technology creators and providers to factor national interest and national security interests in their decision making. As Dr. Galen Hunt said, "Economics is not a justification for creating an insecure world."[29] The Strategy must look for creative ways for private firms and individuals to have national security, in addition to profitability, and be a driver of their business decisions. As an example, when startups are offered capital from nations that are considered adversarial to the United States, firms often may not take into consideration the overall national security picture or the control (direct or indirect) a

---

[27] Kate M. Manuel, et al., "Domestic Content Restrictions: The Buy American Act and Complementary Provisions of Federal Law," *Congressional Research Service*, September 12, 2016, July 3, 2019, https://fas.org/sgp/crs/misc/R43354.pdf.

[28] Defense Acquisition University, "Lowest Price Technically Acceptable," https://www.dau.mil/acquipedia/pages/articledetails.aspx#!484.

[29] Galen Hunt, "Securing the Billions of Devices Around Us." (Keynote Speech at the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019).

nation-state may have over these investors and the business risk their involvement might pose. The Strategy must seek ways to close the gap on the premium adversarial nations will pay over the market because certain technologies may meet their national strategic interests.

- Take steps that increase trust in government resources and intelligence and promote utilization of government-provided intelligence in making business decisions, for example, relating to choosing partners or personnel for positions that require access to sensitive research or data.

A more cohesive community would improve bi-directional information sharing and would allow for the identification and dissemination of best practices. To this end, the Strategy should seek to foster a strong community of technology providers and innovators around issues of mutual concern and benefit. Such a community could help identify actions that, if implemented broadly, would raise the security and prosperity of all. The Government could seek to reward firms who then follow these best practices. A community such as this would allow for the identification and dissemination of best practices or even more formal voluntary norms and constructs. The Enduring Security Framework (ESF) partnership, a cooperative effort organized under DHS' Critical Infrastructure Partnership Advisory Council authority, offers a potential model for how this might operate.[30]

Examples of areas where a strong and self-organized innovation community could have positive impacts might include building a stronger understanding of how participation in industry/governance bodies (e.g., influencing standards development) has both business and national security benefits. Standards bodies abound and are vital to promoting interoperability that enables competition and innovation to thrive across borders. Some examples of standards that have enhanced technology choice and resiliency are included in Appendix C. The increased use of open standards, modular/interoperable networks, open interfaces, and modular design promotes technology choice and supplier diversity and, therefore, enhances resiliency. The Strategy should seek ways to increase understanding of the importance of, as well as participation in, standards development processes. An example is the trend toward O-RANs, discussed further in Appendix A, that facilitate collaboration and spur innovation across borders.[31] Winning the standard is profitable for some, but interoperability means more resilience for all. Transparency and interoperability in standards processes makes it less likely that those processes can be dominated by a foreign-influenced or controlled firm.

[30] Department of Homeland Security, Enduring Security Framework, https://www.dhs.gov/keywords/enduring-security-framework.

[31] Iain Morris, "The Future's Bright, the Future's O-RAN," *LightReading*, June 28, 2018, July 3, 2019, https://www.lightreading.com/mobile/fronthaul-c-ran/the-futures-bright-the-futures-oran/d/d-id/744294

NS/EP-Critical Technologies Face Commercialization Challenges

Many promising technology startups have difficulty surviving until the point where they become viable candidates for funding. This is sometimes referred to as the "Valley of Death." This may be because their addressable markets may not be perceived to be large enough to attract venture funding. The Strategy should examine creative ways to make it easier for startups to thrive outside of traditional venture capital. The Federal Government with its convening abilities may be uniquely positioned to connect the scientific research knowledge base with the communities that can help bring technologies to market and create real-world applications (and thus societal benefits). Some government programs described earlier in this report have been created to do this in order to nurture potentially NS/EP-relevant technologies. Often in these programs, however, decision makers are afraid of supporting a technology that fails to make it to market or for which the desired applications do not materialize. The U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem must orient D/As towards new models in which risk aversion does not stand in the way of supporting promising technologies with unknown future applications. New models must seek to encourage risk, tolerate failure, and shorten the federal investment cycle.[32,33]

Critical Infrastructure Providers

The Strategy should clearly identify actions on the part of critical infrastructure providers that would align with and advance its resiliency and innovation goals. Influencing the actions of this stakeholder group is key because critical infrastructure providers, as the end-users and ultimate consumers of ICT products, represent the demand side of this market, and thus have some level of influence over technology creators and providers. The ESF offers a model for cooperation in this area. The actions desired of this stakeholder group may include: (1) participating in the creation of guidance on how to assess the trustworthiness of ICT products and adherence to such guidance; and (2) implementing product selection criteria that prioritize resilience and security. There are several actions that the U.S. Government could take to drive desired behavior by critical infrastructure providers, including:

- Create awareness and structure incentives so that security and resiliency are elevated as core metrics in their acquisition and sustainment decisions. Critical infrastructure providers must have broad understanding of the inherent value of security and resiliency as well as the tangible business value of trusted technology; ICT providers will in turn respond to the demand.

- Provide better, more timely information to technology users when certain technology providers are deemed untrusted. The NSTAC endorses a recommendation put forward by MITRE to create the National Supply Chain Intelligence Center (NSIC) but recommends this body be broadened in scope and authorities to serve the critical sectors and the emergency preparedness communities (see Section 4.2.3, *Identify Missing Structures and Processes*).

[32] James Lewis, "U.S. Foreign Policy and National Security and Emergency Preparedness Technology Issues." (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, May 9, 2019).

[33] Thilo Hanemann and Daniel Rosen, "China in the ICT Ecosystem," (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, March 12, 2019).

- Create standards to help them assess the trustworthiness of ICT products and avoid, plan for, and mitigate the risks of ICT dependencies (see Section 4.2.3, *Identify Missing Structures and Processes*).

- Evaluate where existing regulatory structures could be improved to elicit desired actions without adding new regulatory burden.

- Work more closely and effectively with, and provide greater value to, industry-facing bodies such as the Information Sharing and Analysis Centers and the Sector Coordinating Councils. Consider how these bodies' impact could be augmented.

Academic Community

The Strategy should first identify the parts of the academic community with which the Senior Advisor should enthusiastically engage, then identify the desired actions by these stakeholders that would advance the resiliency and innovation goals outlined. Finally, the Strategy should identify new methodologies for increasing engagement with all parts of the academic community.

The parts of the academic community that should be engaged include, but are not limited to: material science, systems engineering, computer science, business schools (academics at business schools who address supply chain issues and/or economic issues), and law. Methodologies for increasing engagement with the various parts of the academic community could include:

- Bringing together public, private, and non-profit experts through academic workshops and simulations.

- Encouraging graduate work through fellowships.

- Funding of internships by both the private sector and the U.S. Government.

- Encouraging higher education institutions to provide scholarships for students in the aforementioned areas of science, particularly for students from underserved communities.

- Creating international student exchange programs focused on bringing students from relevant allied countries to engage in learning and dialogue around the issue of ICT resiliency.

- Working more closely with academic institutions to improve personnel vetting for research-related roles.

Finally, the Strategy must consider other methods for supporting academic work and talent creation, for example by using government policies and funding to encourage students to pursue select areas of study, to include potential future employment in national security and critical infrastructure communities. The focus should be on K-12 education to ensure students are fully prepared when they enter higher education in STEM. During K-12, emphasis must be on students' building a solid foundation in the fundamentals of math and science. This is critical to

ensuring a workforce that enables advancements in the critical technologies described in this report and beyond.

Adversaries

The Strategy should clearly identify behaviors on the part of nation-state adversaries that threaten the advancement of the resiliency and innovation goals outlined in the Strategy. In general, the U.S. Government should seek to disincentivize behaviors by adversarial nations that degrade national resiliency and innovation.

There are several actions that could be taken by the U.S. Government that would drive desired behavior by adversarial nations:

- Increasing restrictions on investments in strategic technologies from untrusted parties that would undermine U.S. ICT resiliency.

- Instituting enhanced vetting of applicants from countries with a history of IP theft for work or study visas.

- Advocating for amended conditions of participation in the World Trade Organization that discourage and penalize undesirable actions by other nations.

- Leveraging the dependence of some foreign nations on U.S.-produced components to elicit desired behaviors and discourage undesired behaviors.

An example of a U.S. Government action that is influencing behavior by foreign countries is the passage of FIRRMA, which tightens and expands the scope of review for foreign investment, especially in critical technology sectors. Another example is the *Export Control Reform Act* (ECRA), which requires DOC BIS to lead an interagency, regular process to identify and add to the Export Administration Regulations' export controls list on emerging and foundational technologies that are essential to the national security of the United States. According to analysis by the Rhodium Group, "FIRRMA and ECRA will help address some regulatory gaps but will impair long-term innovation vitality if implemented poorly… There is a risk of overshooting. Trying to shut down 100 percent of inward investment and outbound tech transfer concerns creates its own risk – of choking the positive global interaction spillovers we benefit from."[34] U.S. entrepreneurs desire access to foreign capital, which is sometimes a better, faster option for them than domestic investors, but the United States must restrict foreign nations' access to the most sensitive (or potentially sensitive) NS/EP-critical technology. This is reflected in these recent legislative actions.

[34] Thilo Hanemann and Daniel Rosen, "China in the ICT Ecosystem," (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, March 12, 2019).

4.2.3 Identify Missing Structures and Processes

In addition to identifying the desired actions by known stakeholder groups, the Strategy must also identify agencies and structures that are lacking and must be created.

Standards for Evaluating Risk of ICT

Individual ICT users must make their own risk determination (as part of an overall fitness for use determination) for products they utilize based on a product's intended purpose. NS/EP entities (and all ICT users) need standards to help them assess the trustworthiness of ICT products and avoid, plan for, and mitigate the risks of ICT dependencies.

> "With respect to ensuring we have the ability to assess whether ICT products are trustworthy…We need to evolve the science and the standard."[35]
> *Mr. Donald Davidson, Synopsys, Inc.*

The Senior Advisor will therefore initiate and oversee, in coordination with relevant stakeholders, especially NIST, the development/pursuit of standards to help NS/EP entities assess the trustworthiness of ICT products. These standards should be developed through a public-private process, building upon existing industry standards and/or best practices. The Senior Advisor should consider the work being done in this area by The MITRE Corporation and groups like the Open Group Trusted Technology Forum,[36] and should examine the guidelines for mitigating 5G risk issued by European countries at the Prague 5G Security Conference.[37,38] These standards should be structured to be flexible like the NIST Cybersecurity Framework. They must provide a set of best practices that enable NS/EP entities to assess the risk associated with people, process, and technology, as these contribute to the overall risk of ICT assets. The standards must enable NS/EP entities to assess risk by weighing the criticality of the overall function they perform (considering DHS's NCFs and other forthcoming guidance) and the role of an ICT asset within the enterprise. In addition to technical factors, the standards should also take into consideration the provenance of ICT (chain of ownership of entities producing or touching components including the distribution chain). Standards must be developed in such a way that they do not create the unintended effect of setting a low bar for the methods owners and operators use to evaluate the security and trustworthiness of ICT or to stifle a potentially vibrant market of commercial products to address this challenge.

> "We must direct the creation of better methodologies to evaluate risk present in products, which may include an independent certification methodology, similar to Underwriters Laboratory (UL) certification."
> *Mr. David DeWalt, NSTAC Member and Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee Chair*

---

[35] Donald Davidson, "Cyber-SCRM and 'Commercially Acceptable Global Sourcing Standards'." (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, January 31, 2019).

[36] "A First Step in Securing the Global Technology Supply Chain: Introducing The Open Group Trusted Technology Provider Framework Whitepaper." *The Open Group Blog*, February 9, 2011. https://blog.opengroup.org/2011/02/09/a-first-step-in-securing-the-global-technology-supply-chain-introducing-the-open-group-trusted-technology-provider-framework-whitepaper/.

[37] Government of the Czech Republic, "Prague 5G Security Conference Announces Series of Recommendations: The Prague Proposals," https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[38] Michael Kahn and Jan Lopatka, "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence," *Reuters*, May 3, 2019, July 3, 2019. https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2.

Safe Internet

The challenge to NS/EP ICT resiliency is broader than specific technologies. This was recognized by the NSTAC through the *NSTAC Report to the President on a Cybersecurity Moonshot* as it addressed the need for a safe internet. In that report, the NSTAC illustrated that trusted and untrusted technology, as well as people, are all interconnected as society becomes increasingly dependent on communications networks for daily activities. According to cybersecurity expert Dr. James Lewis, "Originally the internet was looked upon as a frail blossom that we did not want to put too many things on. Today, the functionality of a huge range of mission-supporting devices depends on the core ICT infrastructure and this phenomenon is itself at the heart of the resiliency problem."[39] Then, by extension, the ICT resiliency issue is affected by uncontrollable factors, many of which are unknown until an unintended consequence, or an intended effect from an adversary, is realized. Therefore, to effectively address this problem, it is imperative to address the broader problem of secure and resilient internet connectivity. The Moonshot report recommended the U.S. Government declare a national strategic intent, and empower whole-of-nation resources, to pursue a more fundamentally safe internet environment for critical services. ICT resiliency and supply chain security are fundamental components of this pursuit and this pursuit, in turn, is a vital component of ICT resiliency and supply chain security.[40] The NSTAC reiterates this core tenet of the Cybersecurity Moonshot initiative as a national strategic imperative.

Improved Cross-Sector Engagement

The Senior Advisor will be responsible for coordinating with private sector stakeholders across the COI, which include four main, in some cases overlapping, sub-communities, including: (1) the manufacturing community; (2) the innovation community; (3) the owners and operators of U.S. critical infrastructure; and (4) academia.[41] It will fall to the Senior Advisor to bridge the divide that exists between those private sector communities and U.S. defense and intelligence agencies and federal and emergency preparedness agencies. Limitations on authorities by federal agencies to interact with these private sector agencies exist (often for good reason), and it will also fall to the Senior Advisor to recommend to the President which limitations should remain, which should be amended, and where new limitations may be needed.

To achieve the Strategy's goals for improved cross-sector coordination, the Senior Advisor should:

- Convene and coordinate with key private sector partners within the non-government stakeholder groups, including technology creators and providers, critical infrastructure

[39] James Lewis, "U.S. Foreign Policy and National Security and Emergency Preparedness Technology Issues." (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, May 9, 2019).

[40] NSTAC. *NSTAC Report to the President on a Cybersecurity Moonshot*. (Washington, DC: NSTAC, November 14, 2018) 2018 NSTAC Publications, https://www.dhs.gov/sites/default/files/publications/DRAFT_NSTAC_ReportToThePresidentOnACybersecurityMoonshot_508c.pdf.

[41] The DHS Supply Chain Task Force is in the process of identifying NCFs, which will be useful to the Senior Advisor in identifying the owners and operators who should be included in their plans and programming.

providers, and the academic community, utilizing existing processes already established by federal agencies and federal advisory committees.

- Empower existing bodies and consider where new bodies or public private partnerships (PPP) could fill gaps. The Senior Advisor should look to other areas of government where PPPs have been successful in achieving coordination of efforts between Government and private organizations and achieving unity of mission.

- Change and improve upon existing planning and processes focused on ICT resilience and ensure the ability to operate in degraded conditions and to recover quickly.

PPPs can help provide sectors and the U.S. Government with situational awareness and help them stay ahead of trends in technology and in security risks. As PPPs mature, they can facilitate sharing information between sectors where there are interdependencies, such as those recognized between the telecommunications, financial, and energy sectors in CISA within DHS.

The U.S. Government and the relevant private sector stakeholders should engage in focused discussions in trusted settings about the impediments to engagement regarding forward-looking trends and risks. Congress has acted to foster partnerships and collaboration on cybersecurity threats, as in the *Cybersecurity Information Sharing Act of 2015*, but has not addressed mechanisms to promote the sort of sharing that would be needed to keep the U.S. Government ahead of trends. The Senior Advisor must seek to create, in coordination with the appropriate federal agencies and Congress, the appropriate statutory framework within which companies can provide information on new technologies under development – and their view of the market – without fear that such sensitive business information will be shared with competitors, regulators, or the public.

Enhancing PPPs to address ICT security and resiliency would require some shifts in mindset about information sharing and risk but could be extremely productive. Successful models for PPP cooperation like ESF should be examined and augmented.

Roles of the NSTAC and Other Bodies

The NSTAC was established to provide advice to the President on matters regarding NS/EP telecommunications. The President could seek advice from the NSTAC on matters regarding ICT resiliency and innovation policy as the members represent various entities of that community.

Other important bodies, including the National Infrastructure Advisory Council and the President's Council of Advisors on Science and Technology, can also provide important industry perspectives and information, facilitate cross-sector dialogue, and make recommendations in support of the Senior Advisor and the Strategy.[42,43]

[42] Department of Homeland Security, "National Infrastructure Advisory Council," https://www.dhs.gov/national-infrastructure-advisory-council.

[43] The Networking and Information Technology Research and Development Program, "President's Council of Advisors on Science and Technology (PCAST)," https://www.nitrd.gov/pcast/.

Improved Information Sharing

The MITRE's 2019 report, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in response to the Changing Character of War*, provides excellent recommendations for improving the security and resiliency of the supply chains upon which U.S. warfighting capabilities depend.[44] The report recommends the creation of a NSIC that would serve as a center of excellence for supply chain strategic warning and risk assessment. The MITRE report intends the NSIC to serve as an interagency entity that would aggregate all-source data, both classified and unclassified, cyber and non-cyber, and share it with at-risk operators and industrial partners. The NSTAC endorses this recommendation but believes that the NSIC should be broadened in scope and authorities to serve the critical sectors and the emergency preparedness communities, as well as DOD and IC components and mission owners. If created and authorized with this broader mission, NSIC could become a national resource for threat collection and analysis that produces actionable intelligence and measures that can be utilized across the whole-of-nation (not just whole-of-government as recommended for the NSIC in the MITRE report) at the unclassified level. The responsibilities of this integrated resource could include performing data aggregation and analysis, developing and operating technologies for threat detection, performing risk assessments, generating high-value threat assessments and, through joint interagency interactions, help its members develop measures of risk based on their specific vulnerabilities and mission failure consequences.

4.2.4 Identify and Leverage the United States' Natural Strategic Advantages

Nations that seek to displace the United States as the world's hub for innovation seek to confer advantage on certain companies (national champions) so that they can jump over/bypass some of the challenges to innovation. China directly and indirectly subsidizes such companies, leverages their control over the Chinese economy to support their advancement, and shares with them business intelligence and stolen IP obtained through espionage and its vast government hacking apparatus. China is also unencumbered by public sentiment or market influences: when it wants to direct change it simply does so. One entrepreneur recently described the difficulties the United States faces in nurturing NS/EP-critical technologies, commenting, "China can reprogram its commercial industry whenever it wants to support national objectives."[45] China does not have to generate public support and does not face any public opposition.[46]

Yet the United States has many societal and economic strategic advantages that can be leveraged and strengthened to advance resiliency and foster innovation in the ICT ecosystem. These include, most importantly, the fact that the U.S. economy is market-driven, has a strong, clear, and enforceable legal system (including that which affects IP), a relatively limited degree of government intrusion and regulation, unparalleled financial and higher education systems, and a culture that tolerates and, to some degree, encourages risk taking.

---

[44] MITRE, *Deliver Uncompromised*, https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf.

[45] Tom Foster, "What Happens When A Wildly Ambitious Young Startup Decides to Work With the Military?" *Inc. Magazine*, June 2019.

[46] James Lewis, "U.S. Foreign Policy and National Security and Emergency Preparedness Technology Issues." (Briefing to the NSTAC Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee, Arlington, VA, May 9, 2019).

Other aspects of society that foster innovation include the fact that financial and legal structures permit innovators and entrepreneurs to be nimble and respond to market opportunities. Countries that want to displace the United States in terms of technological innovation have tried to copy and mandate many of these attributes but are having difficulties achieving this in some areas. However, the United States does face some serious impediments in terms of creating and sustaining the societal and economic conditions that foster innovation.

First and foremost, the United States does not invest enough in R&D in basic science and for technologies without a well-defined path to market. The private sector is naturally disincentivized to put resources into these areas. Where the United States does spend funds on R&D, it does so far more effectively than some other nations. The United States' investment in R&D should therefore not be measured dollar for dollar against other nations. Yet there is broad agreement, and the NSTAC enthusiastically agrees, that fostering innovation requires substantially increased financial support from the U.S. Government for R&D as well as specific incentives to private companies to increase their R&D spending. The second major impediment the United States faces for staying on the forefront of innovation is in supporting STEM education throughout all levels of the education system. The *NSTAC Report to the President on a Cybersecurity Moonshot* report underscored the need to "dramatically increase the availability, quality, and diversity of cybersecurity talent for Cybersecurity Moonshot Initiative strategic focus areas," the first of which was technology and innovation. The NSTAC here notes the urgent need for action on this national strategic imperative and reiterates the recommendations relating to STEM education contained in the *Cybersecurity Moonshot* report.

4.2.5 Foster Stronger Cooperation Amongst Like-minded Nations

Like the United States, the governments of many other nations have undertaken many unilateral steps to enhance their national cyber capabilities. The United Kingdom has established a National Cyber Security Centre;[47] France has created its own cyber command[48] and increased its cyber defense budget for the military;[49] Germany likewise has established a Cyber and Information Space Command;[50] and Canada recently passed a bill underscoring the growing role of cyber operations in national security.[51]

---

[47] National Cyber Security Center (NCSC), "About the NCSC," https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

[48] État-major des armées, "La Cyberdéfense au Cœur des Opérations," https://www.defense.gouv.fr/ema/transformation/actualites/la-cyberdefense-au-coeur-des-operations.

[49] Ministère Des Armées "PROJET DE LOI DE PROGRAMMATION MILITAIRE," https://www.defense.gouv.fr/content/download/523150/8769279/file/LPM%202019-2025%20-%20Rapport%20annex%C3%A9.pdf, page 61.

[50] Bundeministerium der Verteidigung, "Entwicklung des Organisationsbereichs bei der Bundeswehr," https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw.

[51] Forty-second Parliament, First Sess., House of Commons of Canada, "An Act Respecting National Security Matters," https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading.

Because ICT is interconnected globally, both from the standpoint of technology production and in the physical sense, it is not possible to address the roots or the impacts of this problem from a unilateral perspective. International engagement is critical. There must be stronger dialogue and coordination among like-minded nations to ensure vibrant, diverse, and trusted global supply chains for ICT products.

The NSTAC recommends that the Senior Advisor, in collaboration with the COI, undertake an analysis of existing international fora and bodies that accommodate and support international engagement on ICT security and resiliency among like-minded nations in order to augment dialogue and coordination among like-minded nations across several key areas:

- Regular engagement amongst relevant government and private sector entities.
- Collaborating on policies relating to ICT security and resiliency.
- Establishing international norms or guidelines for ICT security and resiliency.
- Identifying the need for and ensuring adequate participation in standards-setting activities that are critical to ensuring an adequate supply of trusted technology.
- Supporting shared goals in areas such as supporting scientific research and growing the pool of human capital and talent.
- Coordinating efforts to deter, limit, and act in anticipation of and in response to significant cyber attacks and behaviors by adversaries that threaten global ICT security and resiliency.
- Breaking down international barriers to collaborative innovation.
- Creating more attention and urgency around the issue of ICT security and resiliency within existing international cooperative bodies and alliances.

4.2.6 Advancing the Strategy's Goals

The Senior Advisor must have a whole-of-nation perspective and whole-of-government purview on matters that relate to the resiliency of and innovation relating to NS/EP technologies. In addition, the Senior Advisor must have the ability to compel agencies to take recommended actions as well as to convene private sector stakeholders from the innovation COI. The Senior Advisor will lack operational capacity and therefore will need to execute his or her agenda through an interagency process, relying on resources, including full-time detailees, provided by other federal agencies. These agencies must be aligned behind the Strategy and the Senior Advisor's leadership vision. They must embrace ICT resiliency and innovation not just as an Administration priority, but as a permanent core mission. To accomplish this, the NSTAC recommends several actions, including:

- As part of the Strategy development, the Senior Advisor, in coordination with the OMB Director, shall identify and create the authorities needed by the Senior Advisor to effectively oversee implementation of the Strategy. In doing so, the Senior Advisor and OMB Director

should consider examples elsewhere in the Federal Government authorities that have been effective in convening the appropriate federal agencies and industry stakeholders around national security or national economic objectives.

- As part of the Strategy development, the Senior Advisor will, in coordination with the OMB Director, determine whether D/As will need additional funding and expertise to perform the functions they will be tasked with under the Strategy, and ensure that any needs are met through the budget process. The ability of the Senior Advisor to influence work streams towards specific outcomes within the D/As is not simply a matter of changing the D/A's actions. D/As will need increased funding, manpower, and expertise to fully support the vision of the Senior Advisor and the objectives of the Strategy. The required expertise can be achieved through a combination of organic workforce recruitment and development combined with workforce exchange programs with private sector partners, such as Loaned Executive mentioned earlier in this report. To accomplish the former, D/As performing critical resiliency and innovation roles require excepted service authorities (so-called "pay parity") programs that highly technical D/As, such as the Federal Communications Commission, have utilized to ensure they have a qualified workforce to meet their missions.

- The President should direct the OMB Director, working with Congress, to create a budget function for strategic innovation and resiliency. The NSTAC recognizes that this new budget function would be unique in the sense that it would cut across other existing budget functions, however, its creation would provide a comprehensive view of U.S. federal spending to support resiliency and innovation.[52] It would enable the prioritization of existing funding and would facilitate the monitoring of spending levels for insufficient funding or undesired trends. The NSTAC further recommends that the Senior Advisor be granted the authority to certify that the budget for strategic innovation and resiliency adequately supports and aligns with the Strategy and includes adequate funding in R&D in basic science and for technology development. Funding accounts that should be considered for inclusion in the strategic innovation and resiliency budget function include Government R&D spending and grant programs under DOD, NSF, DOE, DOC, and DHS.

5.0 CONCLUSION

The idea that a foreign adversary would seek to exploit the ICT that the United States procures and willingly utilizes for national defense or critical infrastructure is a deception tactic as old as human history. The security risk posed by ICT products made by potential adversaries is not a new topic in the national consciousness. It is a symptom of the larger problem: that the United States has not adequately prepared for the conditions it is experiencing and will increasingly experience. The internet was never intended to serve as the conduit for almost every business and social transaction, however, it is now just that. Similarly, the Nation did not envision a world in which its critical infrastructure, including basic utilities like power generation and treatment of water, would so thoroughly depend on ICT. Owing to the interconnectedness of this ICT infrastructure and critical infrastructure, the United States has become vulnerable to attack. The advantages of speed, convenience, and flexibility come with an increased attack surface.

[52] House Committee on the Budget, *"Budget Functions,"* https://budget.house.gov/budgets/budget-functions.

Over the past decade, the United States has increased its focus on securing digital communications and the associated privacy considerations. However, most organizations have not paid enough attention to securing the underlying infrastructure (hardware and software) and services that enable these communications. Likewise, the Nation has not given enough collective thought to the possible future technologies these connected networks will enable, their benefits and risks, and the concern that not all such technologies will be created by the United States or trusted partners. It is imperative for the Nation to more carefully consider which emerging technologies to stay on the forefront of even if the margins, valuations, or go-to-market strategy are not as strong as for other products.

The United States needs to do more to foster the success and innovation of U.S.-based companies or those based in allied nations, stopping short of methods that the United States considers anti-competitive and anathema to a core principle of our society. The vibrant innovation community and digital economy the United States is experiencing presents the strongest argument against direct Government involvement in business decision-making. But, in some areas, the United States' hands-off policy has allowed problems to surface. It has resulted in gaps in the Nation's ability to produce some technology and components upon which NS/EP entities depend, or will depend, in the future. The U.S. defense agencies began identifying these gaps years ago and have endeavored, with some success, to address them. Now the Nation is confronting the reality that these same gaps and dependencies also create risk for the providers of the wide array of services upon which all civilian society depends. With vastly greater amounts of ICT infrastructure underpinning these critical services, none of which is owned, controlled, or, in many cases, regulated by the U.S. Government, the problem becomes more challenging. The digitization of critical infrastructure provides benefits to society, not the least of which is safety and efficiency. But it also provides a vector for compromise and potential disruption or destruction of this infrastructure by adversaries.

The path the United States must follow is that of choice and trust. Those responsible for the Nation's NS/EP functions must be able to choose from among several trusted technologies to meet their missions. The United States must avoid dependencies as much as possible, but also strengthen the ability to detect compromise and mitigate impacts. The Nation must advance its resiliency in the sense of ensuring it has multiple providers of ICT, but also in the sense that the delivery of critical services to the public can continue to function should parts of the ICT infrastructure fail or degrade for any reason.

The United States does not need to keep its adversaries out of every ICT component on U.S. networks, but it also should not leave the proverbial doors and windows wide open. The Nation does not need to ban all manufacturers from certain countries, but the United States should restrict the importation and use of some specific products and some vendors that do not follow certain protocols and do not demonstrate independence from foreign nation control. The Nation does not need to try to manage how private companies in the United States make their investment decisions, but it should provide information that can help them be more informed, to better understand the true risks and opportunities. It does not need to share every piece of intelligence with private companies, but it must share strategic intelligence about global supply chain risks in a targeted manner. The United States does not need to shield U.S. companies from competition. Competition is one form of fuel to drive innovation in the United States farther and

faster. But it also does not need to be passive when foreign nations introduce substantial artificialities to create unfair advantages for their own favored companies and industries.

As much as adversaries may seek to exploit the United States' natural shortcomings, the U.S. must leverage its inherent advantages.

This kind of weighing, deciding, coordinating, and convening is what the Senior Advisor must do. The recommendations in this report are all a subset of the recommendations put forward in the *NSTAC Report to the President on a Cybersecurity Moonshot*, which sought to establish a catalyzing framework for collectively tackling complex challenges that pose long-term existential risk. The NSTAC reiterates the concerns and recommendations put forward in that report. With respect to ICT resiliency and innovation, there is a tremendous foundation of work upon which the Nation can build, both from the standpoint of Government efforts and the vibrancy and future potential of its innovation community. It is the responsibility of the Senior Advisor to connect these worlds and coordinate their efforts more comprehensively than is being done today.

The stakeholders identified in this report must acknowledge that the economic and societal choices made to date leave the United States susceptible to exploitation by adversaries. Following the whole-of-nation recommendations from the *Cybersecurity Moonshot* report and the specific recommendations relating to ICT resiliency and innovation advanced in this report, the Nation's communications infrastructure can be resilient now and, in the future, while the norms and values that make U.S. society and economy thrive remain unchanged.

APPENDIX A: 5G CASE STUDY

I. EXECUTIVE SUMMARY

Evolution of 5G Technology

Fifth generation (5G) technology is the next generation of wireless communications technology building upon and succeeding fourth generation/long term evolution (4G/LTE). 5G networks enable significantly faster speeds, lower latency, and greater component functionality. Moreover, 5G will enable a range of applications. Multiple studies have indicated that 5G networks will enable applications to drive significant technological advances and add $500 billion to U.S. gross domestic product and three million jobs.[1] As a result, the next age of digital transformation depends on the success of the 5G build out in the United States.

5G technology has developed at the same time as an ongoing shift in networks from hardware to software, embracing concepts such as software-defined networking (SDN) and network function virtualization (NFV). The introduction of information technology infrastructure and cloud computing concepts into the mobility network, enabling developments such as mobile edge computing, may provide an option to address supply chain concerns by driving the industry toward a more interoperable, modular network design that will foster competition between suppliers and lower barriers to entry for new entrants in the marketplace.

At the same time, as industry transitions from centralized core and radio access networks (RAN) to distributed, virtual, and more open networks, networks will have more agile and layered security. Industry made significant strides to address security in LTE networks, and now industry is building in additional capabilities, such as stronger encryption and embedded protections from Distributed Denial of Service attacks, across the network. A recent report from the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) lays out in detail the evolution of 5G and the security opportunities and risks that attend 5G deployment.[2] The CSRIC concluded that there is no single solution to ensure the security of future telecommunications networks, but there is a great deal of promise.

Supply Chain Challenges

As discussed in the *NSTAC Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*, there are concerns about the growing presence of Chinese telecommunications equipment manufacturers, particularly in networks outside of the United States, and the long-term implications for 5G and the broader communications and internet technology supply chain. This concern is particularly acute in the RAN portion of the network where there are a limited number of RAN equipment suppliers.

[1] Accenture,"New Research from Accenture Strategy highlights Economic and Societal Impact of Investing in 5G Infrastructure," https://newsroom.accenture.com/news/new-research-from-accenture-strategy-highlights-economic-and-societal-impact-of-investing-in-5g-infrastructure.htm.

[2] Federal Communications Commission, Communications Security, Reliability and Interoperability Council, Working Group 3, "Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks," www.fcc.gov/files/csric6wg3sept18report5gdocx-0.

A primary concern is the growing presence of subsidized competition from China. If Chinese manufacturers continue to gain market share, there is growing concern about the long-term viability of the existing supply chain for 5G and successor technologies. The consolidation of vendors has decreased vendor diversity and created challenges for new entrants. Upfront costs related to labor, equipment, and research and development (R&D) all work to discourage new communications vendors from competing with established players. However, there are opportunities to correct this in the future. This appendix will discuss several aspects of a tightening supply chain, including:

- Consolidation of vendors;
- Decline in vendor diversity;
- Effects of consolidation on U.S. network advances; and
- Opportunities to improve technology choices.

The Role of Government

Finally, this appendix provides insight into the 5G landscape and recommendations to the U.S. Government for methods to stimulate the U.S. role in the 5G ecosystem. Government officials should consider what led to a lack of domestic development of network infrastructure suppliers in the wireless space. Government has several essential roles to play, to bring more diverse vendors into the supply chain.

Short-Term Policies

- **Promote Vendor Diversity.** Persuade allied governments to reduce or eliminate dependency on single-supplier equipment, provide incentives for European Open-RAN (O-RAN) vendors to move R&D to the United States, encourage new start-ups in O-RAN development, and encourage formation of an equipment consortium to promote more open and secure 5G network design.
- **Encourage Use of Open Standards in RANs and Enhanced Interoperability.** Strongly encourage O-RAN platforms and carrier adoption of such technologies with real incentives to carriers to deploy multi-vendor, interoperable solutions.
- **Foster Participation in Standards Setting.** Provide tax incentives and other encouragement for expanded participation by U.S. companies and academics in the Third Generation Partnership Project (3GPP) and other standards bodies. Create opportunities for policy makers to gain expertise in and increase support for global standards developments.
- **Incentivize the Adoption of U.S. Technology**. Government can also develop incentives for the adoption and use of U.S.-based technology by both the public and private sectors.
- **Expedite 5G Deployment and Collaboration.** Eliminate barriers to wireless deployment by supporting small cell deployment and making more spectrum available for commercial use.

- **Manage an Overall Government 5G Strategy.** Create or name a government entity responsible to manage an overall government 5G strategy with cross-sector engagement that encompasses the short- and long-term recommendations in this appendix.

Long-Term Policies

- **Create Vital Economic Incentives.** Develop incentives such as tax policy, including tax credits, as incentives for private sector innovations in the 5G ecosystem and R&D and standards activity.

- **Incentivize Industry Action.** Incentivize industry action toward more diverse and resilient supply chains, support long-term industry strategic planning around supply chain resiliency, and provide significant incentives to European and Western O-RAN vendors to move their R&D resources and facilities to the United States and to develop solutions to the U.S. market.

- **Strengthen Expertise and Innovation.** Grant scholarships and other educational incentives to Americans to study wireless technologies, software engineering and cybersecurity in the wireless space and retain wireless and cybersecurity experts to participate directly or through academic institutions in open software forums. Encourage U.S. entities to promote wireless innovations for post-5G developments.

- **Protect Intellectual Property (IP) and Use Import Controls.** Advocate for aggressive protection of U.S. technology IP rights and use import controls as necessary to support the availability of domestic sources for a diverse 5G supply chain.

II. 5G OVERVIEW

5G Network Technology and Capabilities

5G is the fifth generation of wireless technology. It will be the most robust wireless communication technology deployed to date and will enable faster and more powerful networks, and a dramatic change in how society lives, works, and plays. Smart cities, autonomous cars, industrial Internet of Things (IoT), connected health care, and distance education will rely on the 5G network's ultrafast speeds, massive device connectivity, ultra-reliability, ultra-low latency, and better capacity and coverage.

5G is not brand new. It is not a flash cut technology. 5G will build on the existing, robust LTE and LTE-Advanced technology and infrastructure that has made the United States a global leader in technology and connectivity. There are significant characteristic and architectural differences between 5G and 4G LTE, impacting the RAN, Core, and Edge. The 5G RAN supports a new, larger antenna array known as Massive Multiple Input Multiple Output, and the 5G RAN components are decoupled and distributed. The 5G core network features new design configurations to support the unique 5G services. In addition, 5G introduces a new network segment, the mobile edge, to enable next generation ultra-low latency and high bandwidth applications. The mobile edge includes elements traditionally part of the RAN and Mobile Core.[3]

[3] SDxCentral, "What is Edge Computing?" https://www.sdxcentral.com/edge/definitions/what-multi-access-edge-computing-mec/.

Higher Speeds. Peak 5G network speeds will be approximately 20 times faster than 4G. Increased network speed, based on additional bandwidth and data transfer rates, stems from additional capacity and much wider spectrum channels across more frequencies than 4G was designed for. 5G can address channels as wide as 200-400 megahertz (MHz), a ten times increase in capacity of the wireless signal. To leverage these wider bands, additional spectrum must be freed across lower-, mid-, and high-band spectrum.

Lower Latency. Latency, the time it takes to send a packet of data, will be significantly lower in 5G networks. 5G's lower latency is a function of a smaller and more efficient network frames or packets, including changes to the control layer that affects network scheduling to minimize wait time before a request is picked up.

Other Technology Advances. Another 5G technology improvement, known as Lean Carrier, allows the carrier to choose not to send many of the signaling and redundant data packets that historically have been required in 4G. As a result, speed and service quality improve for mobile users. 5G can support more devices per square mile, which is of benefit to IoT.

Standards Setting. Global standards are critical for interoperability between networks and devices. Standards foster the economies of scale needed for global development of new technology. Standards development organizations (SDO) are critically important to the technical trajectory of 5G; an increased presence by American companies and experts is vital. The global telecommunications ecosystem has a history of collaborating on standards. This is not a government-driven process. It is left to private experts—engineers, scientists, and other builders—to debate problems and solutions, working toward consensus in a transparent way. All countries and companies must wait for the same standards to be developed to manufacture equipment and deploy 5G. Any non-standard deployment will not be scalable or interoperable with other networks.

3GPP is the main standards body developing 5G. As standards evolve, 5G technology will transform networks and operations. Wireless technology evolves as features are introduced by 3GPP via releases. This has been done since 2G. Releases are not rigidly timed, and work is done on multiple releases simultaneously, in phases. When a release is finished, it indicates that new features are ready for implementation by carriers and manufacturers around the world. Releases are iterative, in that they build on previous releases. The 5G process has more input than past specifications because operators and manufacturers recognize the importance of contributing to a global standard. Hundreds of companies and organizations participate in 3GPP to vet contributions and develop standards. The process is driven by engineers, which supports technically sound ideas and standards.

SDN and NFV. Traditionally, telecommunications operators have built networks by interconnecting components that provide various network functions, including switches, routers, access nodes, multiplexors, and gateways. Most of these network functions were implemented as integrated and closed systems – unique hardware tightly bundled with unique and inseparable software, along with a vendor-specific management and automation system. For operational ease, network operators traditionally would use one or two vendors for a given class of network components. Since most deployed network hardware components are seldom replaced, this

creates vendor lock-in for both hardware and software, with limited options for upgrading as technology advances.

In the last decade, this paradigm has begun to change as network operators move from a hardware centric network design methodology to one that is software centric. In this new model, the hardware consists of standardized and commoditized white boxes (e.g., cloud hardware), which can be independently selected and upgraded to benefit from technology advances. The network function capability is largely implemented in independent separate software running on commodity white box hardware. The same hardware can support multiple network functions, which are implemented through software components as virtual network functions running on the white box hardware. This software-based approach allows network operators to scale their networks to match demand and ensures maximum utilization of network resources.

The move to a software-based construct requires disaggregation of the telecommunications hardware and software and enables a high degree of operational automation. In 2017, more than 50 of the largest network and cloud operators representing 70 percent of the world's mobile subscribers, including from China, formed the Open Network Automation Platform (ONAP) project to deliver an open, standards-driven architecture and implementation platform.[4] ONAP seeks to rapidly instantiate and automate new services and support complete lifecycle management of these software-based virtual network functions. As a result, operators can leverage their existing network investments while accelerating the development of a vibrant virtual network function ecosystem.[5]

ONAP enables several key capabilities including: (1) independent management of applications, networking and physical infrastructure; (2) a service creation environment that is not limited by a fixed underlying network or compute infrastructure; (3) the automatic instantiation and scaling of components based on real time usage; (4) the efficient reuse of modular application logic; (5) automatic configuration of network connectivity via SDN; and (6) user definable services.

Trend Toward Openness in the RAN. These same developments are now occurring in the radio access portion of the network led by the O-RAN Alliance.[6] The radio access portion of wireless networks contains wireless base stations, known as Evolved Node B (eNodeBs or eNBs), which are connected to each other and to the Enhanced Packet Core network.[7] There are multiple components within each base station, most importantly the radio remote unit (at the antenna) and the baseband unit. These components are typically connected by fiber and interoperate via a front haul interface, the Common Public Radio Interface.[8]

In traditional wireless RAN deployments, vendors maintain key connections as proprietary/closed interfaces. For example, in the past an Ericsson component (such as a radio) could not communicate with a Nokia component (such as a baseband unit), and individual

[4] Linux Foundation Project, "Open Network Automation Platform," https://www.onap.org/about.

[5] *Ibid.*

[6] Iain Morris, "The Future's Bright, the Future's O-RAN," LightReading, June 28, 2018, July 3, 2019, https://www.lightreading.com/mobile/fronthaul-c-ran/the-futures-bright-the-futures-O-RAN/d/d-id/744294.

[7] AT&T Developer Program, "Long Term Evolution," https://developer.att.com/technical-library/network-technologies/long-term-evolution.

[8] Common Public Radio Interface, "Industry Leaders Releasing the New eCPRI Specification for 5G – eCPRI V 2.0 with Additional Functionality for Interworking," http://www.cpri.info/press.html.

eNodeBs from one vendor would have limited interoperability with eNodeBs from another vendor. This required network operators to build networks with fully integrated solutions from a single vendor. Thus, while many operators use multiple RAN suppliers, the operators typically needed to build with single vendor's equipment in any given geographic area.

O-RAN seeks to open and standardize these interfaces and move from dedicated proprietary hardware to white box hardware. This would allow different vendors to provide radio units, baseband units, and backhaul, and for network operators to shift to modular networks with different components and software sourced from different suppliers. A large component of the baseband unit is already software-based, but today the functions are combined into single units from a given supplier.[9] By shifting to commoditized white box hardware, O-RAN is striving to decouple the baseband unit software from the hardware.[10] As of April 2019, 19 network operators and over 60 suppliers support O-RAN.

III. THE CHALLENGE OF SHRINKING 5G SUPPLY CHAINS

Policymakers and industry are both concerned about the 5G supply chain, both in terms of its breadth and diversity and its reliability and trustworthiness. Several dynamics have led to a concentration in the manufacturers that contribute to the 5G ecosystem, with geopolitical, diplomatic, and economic security implications. It is important to understand the dynamics of how the ecosystem got to this point to identify productive policy steps that government can take to expand the diversity and resiliency of supply chains.

Consolidation of Vendors. Several challenges must be addressed to maintain the dominance of the United States, its allies, and U.S. companies in the communications sector. A major challenge today is ensuring a diverse, competitive supply chain in the face of increasing industrial strategies and policies from China, which has resulted in a consolidation of vendors. According to the Mobile Infrastructure Market Tracker survey by IHS Markit, Huawei surpassed Ericsson in 2017 for the lead in the overall infrastructure market with 28 percent market share compared to 27 percent for Ericsson, 23 percent for Nokia, and 13 percent for ZTE. This means that Chinese suppliers were over 40 percent combined, compared with the European suppliers.

The trends in market share are even more concerning. Based upon IHS Markit Data, Chinese manufacturers have grown from less than 10 percent market share worldwide in 2010 to approximately 38 percent in 2018, an increase of four times.[11] Part of this is due to the 77 percent share Chinese manufacturers hold in China alone, the world's largest market. However, Chinese manufacturers have grown from 3 percent in 2010 to over 46 percent in 2018 in the Asia Pacific region, and from 17 percent to 30 percent in Europe. At the same time, the market share of Chinese manufacturers has only dropped from 1.5 percent to 0.2 percent in the United States. In its briefing to the NSTAC, the National Telecommunications and Information Administration

---

[9] Linda Hardesty, "O-RAN Aims to Eliminate Vendor Lock-in at the Radio Access Network," *FierceWireless*, March 19, 2019, Last Accessed July 9, 2019, https://www.fiercewireless.com/wireless/o-ran-aims-to-eliminate-vendor-lock-at-radio-access-network.

[10] *Ibid.*

[11] Thomas Swanabori, "Spectrum, 5G networks, and Cybersecurity." (Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 18, 2019).

also presented similar data demonstrating that Huawei has recently surpassed Ericsson as the largest global provider of base station sales in 2017.

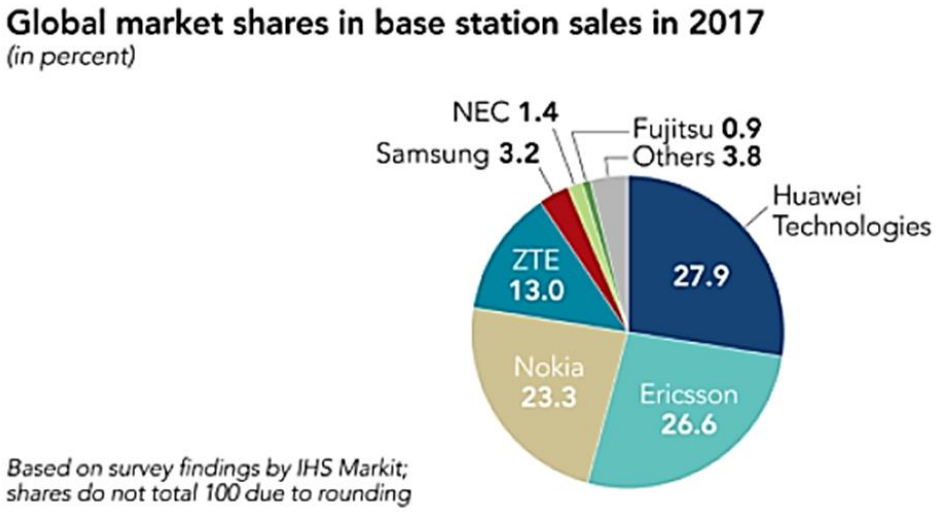

Figure A-1: *Global Market Shares in Base Station Sales in 2017*[12]

[12] Evelyn Remaley and Diane Rinaldo, "5G Market Dependencies and Complexities." (Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 26, 2019).

The Center for Strategic and International Studies (CSIS) also published a report in December 2018 further elaborating on these challenges.[13] CSIS breaks down the network between user equipment, the RAN, and the Core Network. The following chart is an excerpt from the CSIS report indicating market share in each of these areas:

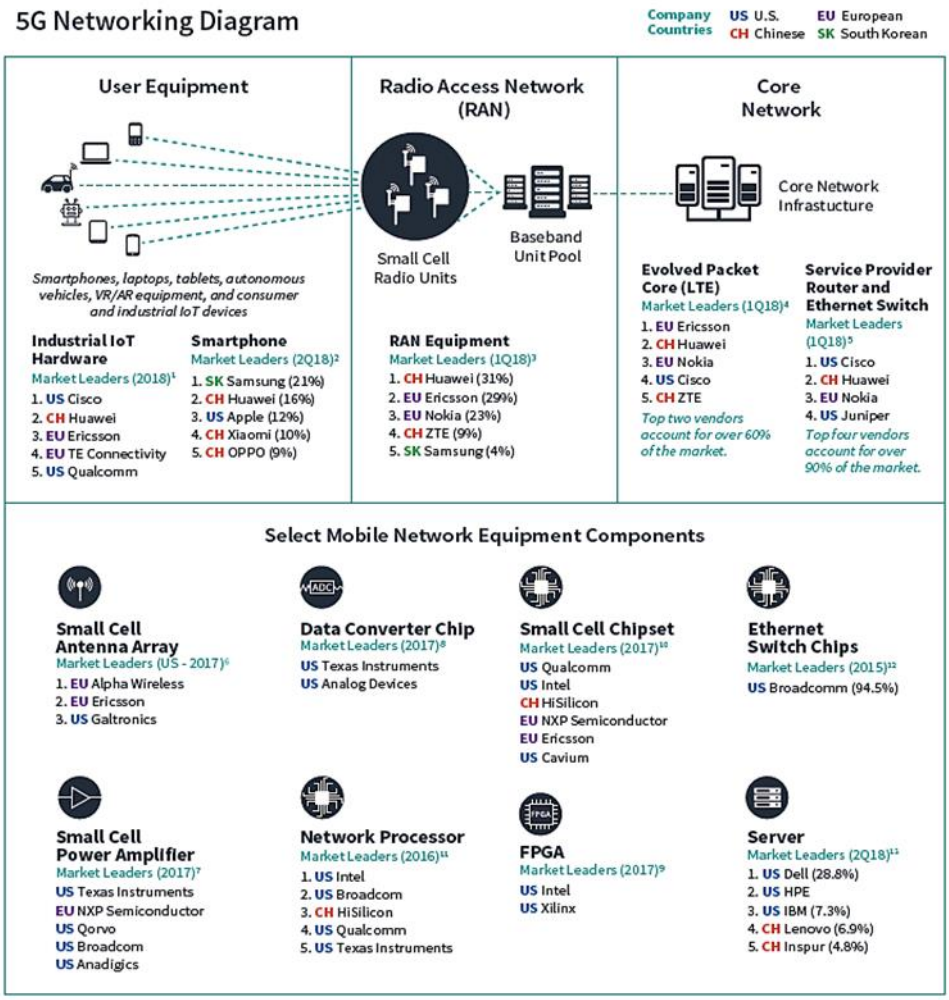

Figure A-2: *5G Networking Diagram and Select Mobile Network Equipment Components*[14]

The principal concern is that, over time, continued growth by Chinese manufacturers may crowd out alternative options resulting in more limited market alternatives. This possibility already exists with respect to R&D spending. Huawei has been reported to have spent $13.8 billion in R&D in 2017 compared with just $4.5 billion for Ericsson and $5.2 billion for Nokia.[15] This

[13] James Lewis, "How Will 5G Shape Innovation and Security: A Primer," Center for Strategic and International Studies, December 6, 2018, Last Accessed July 10, 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.

[14] *Ibid.*

[15] Iain Morris, "Huawei Dwarfs Ericsson, Nokia on R&D Spend in 2017," LightReading, April 3, 2018, July 24, 2019, https://www.lightreading.com/artificial-intelligence-machine-learning/huawei-dwarfs-ericsson-nokia-on-randd-spend-in-2017/d/d-id/741944.

trajectory will not maintain a vibrant marketplace, and policymakers must actively look at means to encourage a long-term diverse supply chain.

Factors Driving Decreases in Vendor Diversity

Various factors contribute to a decrease in vendor diversity. Revenues are dwindling due to decline in demand from mobile telecommunications operators and price pressure from Asian competitors. In the case of China, low labor costs have enabled tremendous cost advantages. This economic scenario led to massive restructuring initiatives that resulted in consolidation in RAN technology industry in Europe and Asia. New players faced often insurmountable barriers to entry.

Competition from Chinese companies, Huawei Technologies and ZTE Corporation, and to a lesser extent South Korea's Samsung, has remained fierce for many years, leading to continued erosion of European vendors' mobile infrastructure market share.

Standard and Poor's Financial Services 2017 reporting illustrated ongoing market share declines from Ericsson with Huawei surpassing them as the leading provider of mobile equipment in 2015.

Due to the magnitude of investment required for a network build, mobile providers often enter agreements with a limited number of established infrastructure vendors to manage risk and guarantee continued support. Such an approach can constrain the adoption of emerging technologies developed by startups.

Effects of Consolidation on U.S. Network Advances

The consolidation of vendors is also impacting U.S. networks. The development of RAN capabilities has been driven from outside the United States, for example, in Sweden, Finland, and China. Recreating the experience and knowledge base in the United States will take many years and significant investment. Vendor consolidation and the prominence of vendors from China have raised security issues. In addition to concerns about vendor-installed backdoors, security issues could be introduced through poor software development practices both during and after the rollout of 5G.

As Chinese suppliers continue to gain share in the telecommunications equipment market, there is growing concern by policymakers and industry that China will crowd out alternative options. As noted previously, this outcome would have a significant impact on many of the new technology advances anticipated in the future that will rely upon advanced 5G networks.

A shift to O-RAN platforms could help address certain aspects of these trends, but it must be complemented by government-led policy changes. The trajectory of Chinese manufacturers crowding out alternatives is not a foregone conclusion, and policymakers and industry can take steps to maintain a vibrant marketplace and encourage a long-term diverse supply chain.

Future Opportunities to Improve Technology Choices

Over time, shifting to an open design framework, through efforts such as O-RAN, can expand the number of suppliers, promote the long-term viability of the supply chain, and prevent dependence upon a single vendor.

Why do these developments in networking matter for the supply chain policy challenges outlined above? Simply put, the long-term viability of the supply chain can be supported by embracing a more open, modular, and interoperable design. As a result, network operators will not have to rely on a single vendor offering fully integrated solutions based on proprietary designs. The approach will also lower barriers to entry in the marketplace because suppliers will not be forced to build fully integrated systems and will be able to innovate in areas of competitive advantage. The migration to virtualized network functions should open opportunities for companies that excel at software design that may previously have been closed to them.

These developments will also shift value from proprietary network hardware boxes to network components and integrated circuits where U.S. and European suppliers have a major market presence as illustrated in the CSIS table above. In a more modular design, a new entrant can focus on specific aspects of the RAN. An example of this could be in active antenna array technology. If a supplier innovates in active antenna array technology, a network operator could more quickly deploy the new antenna array technology on existing infrastructure because upgrading the baseband units simply would be a software upgrade on commoditized hardware.

Also, the shift to software driven networks should reduce the cost of entry for creating network applications and decoupling the hardware from the software and give network operators more options for low-cost and less complex hardware. The migration to modular, software-defined networks should also enable operators more effectively to scale their networks to meet future use cases, applications, and other demands.

O-RAN demonstrated what this future could look like at Mobile World Congress in early 2019. O-RAN showcased a mmWave radio unit transmitting a 5G new radio signal with 100MHz bandwidth using a 5G open RAN test platform and a 28 gigahertz open radio unit white box. AT&T, Anokiwave, Ball Aerospace, Xilinx, and Keysight Technologies – all U.S.-based firms – sponsored the demonstration and provided the underlying components in a white box design. Another example of the software-based approach includes suppliers such as Altiostar, which is collaborating with Rakuten on its 5G wireless infrastructure.[16]

The shift to a more open, interoperable or white box design is also critical to enabling the greater future use cases and applications that will depend upon the network infrastructure. More diverse suppliers and market participants will lower overall costs and enable network operators to scale more efficiently to meet the ever-increasing demands on future core networks. It will create opportunities for the entry of new vendors, including those in the United States, in strategic niches and could alleviate some security concerns.

[16] Linda Hardesty, "Cisco's Early Bet on RAN Virtualization Propels Altiostar," *FierceWireless*, May 19, 2019, Last Accessed July 9, 2019, https://www.fiercewireless.com/tech/cisco-s-early-bet-ran-virtualization-propels-altiostar.

IV. THE ESSENTIAL SUPPORTING ROLE OF THE GOVERNMENT

The United States is leading the push to 5G with investment and smart spectrum policy, building on robust infrastructure that was fostered by a light-touch regulatory environment. The Federal Government can help maintain this global leadership by removing barriers and promoting infrastructure deployment and incentivizing and encouraging actions by industry and other stakeholders.

A popular talking point is that the United States is at risk of losing the race to 5G deployment. Such statements give inadequate attention to the great strides U.S. operators and the Government are making to advance 5G. Some policymakers suggest the United States can "win" by nationalizing communications infrastructure or adopting a top-down approach to growing private, heterogeneous networks. But this approach would slow, not advance, national objectives and remove the biggest advantages the United States has in the race: robust competition and light-touch regulations, both of which spur world-leading innovation and investment.

Policymakers can take steps to reinvigorate the 5G marketplace and promote a more diverse and secure environment. While the U.S. Government is continuing to push for policies the mitigate the concerns around the growth of Chinese suppliers, the short- and long-term policy actions outlined below can support the future integrity of the supply chain and should be considered by the Senior Advisor in the development of the U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem.

Short-Term Policies

Promote Vendor Diversity. In the United States and other countries, it is paramount to ensure that no single vendor dominates network infrastructure. For example, the United Kingdom has divided core 5G networks and RAN vendors between Huawei, Ericsson, and Nokia. Vendor diversification will improve resilience and security by ensuring that the networks are not dependent upon any one vendor and will help ensure that a range of options remains viable into the future. Key actions may include efforts to:

- Persuade allied governments to reduce or eliminate the dependency on single-supplier network equipment and increase demand for supply diversity;

- Provide significant incentives to European O-RAN vendors to move their R&D resources/facilities to the United States and develop solutions for the U.S. market; and

- Encourage new startups in O-RAN space and provide carriers with tax incentives for using platforms developed by U.S.-based vendors.

Encourage Use of Open Standards in RANs and Enhanced Interoperability. Policymakers should strongly encourage O-RAN platforms and carrier adoption of such technologies with real incentives to carriers to deploy multi-vendor O-RAN solutions. The continued migration to SDN/NFV will support more open, interoperable networks enabling networks to scale to meet increasing demands from the technologies that will be powered by 5G, such as IoT.

Industry alliances, such as the O-RAN Alliance and ONAP, are driving developments to support this vision of the future. Presently, 19 carriers and more than 60 vendors are members of the O-RAN Alliance. Policymakers should encourage vendors to embrace O-RANs and open, interoperable, international standards. This approach will enable network operators to build networks on a more modular basis with components from multiple suppliers interoperating with one another. In addition, it will enable network operators to lower barriers to entry as hardware becomes more commoditized and networks become increasingly software-based, as well as prevent vendor lock-in that will compound these challenges in future generations of wireless technology. Government policies should also encourage seamless interoperation between the 4G and 5G networks of different vendors.

Foster Participation in Standards Setting. Global standards for wireless telecommunications are critical for interoperability between networks and devices. They foster the economies of scale needed for global development of new technology. As people, data, and devices cross borders with increasing fluidity, there must be neutral and common technical approaches that allow interconnection and predictable interfaces. The benefits of global standards can be seen with today's 4G networks. The majority of the world's wireless services are built on the same global technology standard, and customers can therefore make calls and access data in hundreds of countries across the globe.

Perhaps the most effective endorsement of global standards is a cautionary tale of the pitfalls of eschewing them. With past generations of wireless technologies, some companies launched proprietary technology in a race to be first, only to have to backtrack later, leaving their customers with potentially obsolete equipment. In contrast, 5G will be built on global consensus standards and specifications informed by almost 600 organizations working to meet international expectations.

The Government can foster participation by U.S. companies and academics in the 3GPP standards body and other technical venues. 3GPP is an umbrella standards body that draws on seven organizational partners from Asia, Europe, and North America. These are regional accredited SDOs that have as their members wireless carriers, equipment manufacturers, and other stakeholders. Companies contribute to 3GPP as individual members via their membership in a participating organization partner. There are currently 588 members in 3GPP, and the Alliance for Telecommunications Industry Solutions (ATIS) is the North American founding organizational partner of 3GPP.

3GPP operates under detailed procedural rules to ensure regional balance and transparency. Hundreds of members work through seven organizational partners. The work in 3GPP is done in various working groups that formed under Technical Specification Groups (TSGs). Each TSG is led by a Chair and Vice Chairs elected by the membership, with term limits and regional diversity requirements. 3GPP has three TSGs: RANs; Service & Systems Aspects; and Core Systems and Terminals.

To amplify leadership in standards, additional North American organizations can become contributing standards members. Standards development driven by the private sector with robust participation will support U.S. technological leadership for the next decade. Importantly, it will transfer institutional knowledge as longstanding corporate representatives train junior experts to

carry forward this work. This is particularly important as standards work relies on relationships of trust built on shared expertise and collaboration.

It also would be beneficial for policymakers to have opportunities to gain full understanding of the nature and purpose of global technology standards activities, as background to lending greater support in this area. Programs to accomplish this could be organized between private sector experts who participate in standards development and the U.S. Government technical technology experts.

The U.S. Government could provide tax incentives for participation in standards bodies and demonstration of significant R&D contributions in the wireless space. This would ensure greater participation in standards setting bodies by U.S. companies and researchers.

Incentivize the Adoption of U.S. Technology. Government can also develop incentives for the adoption and use of U.S. based technology by both the public and private sectors. It won't be enough to invest in standards participation and to encourage new entrants in the marketplace through open and interoperable networks. The U.S. Government should investigate how to actively encourage firms to use U.S. or allied technology and partner with other nations to create the necessary scale and market opportunity to enable these businesses to thrive in the future.

Expedite 5G Deployment and Collaboration. Policymakers should continue to eliminate barriers to wireless deployment by supporting small cell deployment and making more spectrum available for commercial use. The Federal Government can encourage Government adoption to further incentivize 5G deployment. The FCC has taken some steps in this direction with shot clocks to govern local review of siting requests. In addition, recent EO directed federal property managing agencies to accelerate the deployment and adoption of affordable, reliable, modern high-speed broadband connectivity in rural America. The FCC also plans to move forward with auctions of mmWave spectrum later this year.

Manage an Overall Government 5G Strategy. The scope of activities required to support 5G is complex and involves cross-sector engagement by numerous government D/As and private sector players. The Government should have an entity to manage an overall 5G strategy that encompasses the short- and long-term recommendations in this appendix.

Long-Term Policies. Over the longer term, policymakers should take the short-term recommendations to another level and develop additional policies to help improve vendor diversity and address other 5G challenges on a truly transformative and sustained basis.

Create Vital Economic Incentives. As part of its longer-term strategy, the Government can provide incentives to augment participation by U.S. companies and academics in standards bodies and open software forums to foster innovation in NS/EP-critical ICT by companies from the United States and allied countries.

Investment in R&D inevitably drives future releases of global standards work. As many western countries are cutting back on government-encouraged R&D, China is making substantial investments. The United States should carefully consider what role it wants domestic industry and innovation to play in long-term technology leadership and standards development, and how to ensure that meaningful incentives for R&D are in place.

As noted in the short-term policy discussion above, tax policy, including tax credits, could create powerful incentives for private sector innovation in the 5G ecosystem including R&D and participation in standards activity.

Incentivize Industry Action. The U.S. Government can play an important supporting role in incentivizing industry actions that increase vendor diversity throughout the 5G supply chain. The Government can undertake initiatives that support the adoption of U.S. technologies across both the private and public sectors. Policymakers can also encourage different sectors of the U.S. Government to sponsor the use of new wireless technologies that build on successfully deployed 5G networks. Policies should be developed to provide significant incentives for European RAN vendors to move their R&D resources/facilities to the United States and to develop solutions for the U.S. market.

Strengthen Expertise and Innovation. Extensive expertise is required to maintain U.S. global technology leadership, participate heavily in global standards development, and implement a shift toward greater diversity and 5G network models and capabilities. Scholarships and other education incentives encouraging more Americans to study wireless technologies, software engineering, and cybersecurity will be key to expanding the U.S. pool of expertise around 5G networks and, with it, the extraordinary capabilities of these new technologies.

The U.S. Government should retain wireless and cybersecurity experts to participate directly or through academic institutions in open software forums. Policymakers should encourage the many relevant components of the U.S. Government to promote innovations of new wireless technologies building on successfully deployed 5G networks.

Protect IP and Use Import Controls. The U.S. Government should advocate for aggressive protection of U.S. technology IP rights to benefit U.S. companies directly and slow down China's efforts to dominate the telecommunications ecosystem. Import controls can be leveraged to slow the rate of market loss for domestic suppliers. Trade policies should be adjusted as necessary to discourage vulnerabilities in supply chains that put national security assets and missions at risk. Economic sanctions should be considered for companies with a history of selling products with documented backdoors and security vulnerabilities.

APPENDIX B: STRONG U.S. SEMICONDUCTOR INDUSTRY CRITICAL TO ICT RESILIENCY

The semiconductor industry provides an example of a highly critical technology in which the U.S. leadership position is threatened by several factors. Today, the world depends on U.S. designed and manufactured semiconductors to power their economies. However, market conditions are changing as China and other nations have made a strategic decision to build a domestic semiconductor industry supported by massive subsidies. If this continues unchecked, it will disrupt U.S. industry's ability to compete and the United States could become reliant on foreign-based companies to meet its needs for semiconductors and/or next-generation semiconductor technology.

Since World War II, the United States has been the dominant world leader in semiconductor research, design, manufacturing, and innovation. This has enabled transformative leaps in modern national security and emergency preparedness information and communication technology (ICT) and formed the core of emerging technologies including artificial intelligence, autonomous vehicles, quantum computing, and advanced wireless networks including fifth generation (5G).

However, continued innovation in the sector is being challenged by factors emerging from both science and geopolitics. Scientifically, the laws of physics have begun to push the boundaries of Moore's Law, which may require the use of alternative materials to silicon and novel design ideas to make computers faster and more powerful.

In 2015, the Chinese government announced a national plan to catch up to the United States in semiconductor technology and invest more than $100 million to build new fabs and foundries. China still trails U.S. semiconductor companies in science and engineering-based innovation, with U.S. industry maintaining its edge for now. However, due to the massive capital expenditures required to maintain and modernize semiconductor manufacturing facilities and the sales volume required to generate profits, the size and scale of China's investment could eventually compromise the ability of U.S.-based manufacturers to compete globally, posing a risk to U.S. economic and national security. What it has not been able to develop domestically, China has sought to acquire internationally. To date, Chinese firms and sovereign wealth funds have been prevented from buying controlling stakes in U.S. firms through the Committee on Foreign Investment in the United States and other U.S. legal authorities.

Further increasing the pressure on the industry is an aging workforce that is not being adequately backfilled to support growth and competition from China and other countries for talent. The U.S. semiconductor industry's advantage in innovation depends on the efforts of scientists and engineers to design and manufacture products that are better than foreign competitors. The number of American university students graduating with degrees in computer science, electrical engineering, and materials science and going into the semiconductor industry is not nearly enough to support the current demand of U.S. companies. Compounding this problem, experienced engineers and scientists employed by U.S. companies in design, operations, and research are being recruited to join foreign-based companies with compensation offers that double or triple their current income. U.S. immigration policy further hinders the industry by discouraging or prohibiting graduate students in these disciplines, who are primarily foreign nationals, from remaining in the United States.

This is not the first time that challenges to the semiconductor industry threatened national security and triggered a response. In the 1980s, the U.S. Government and industry joined forces to form the Semiconductor Manufacturing Technology Consortium (SEMATECH) Consortium, whose purpose was to maintain U.S. semiconductor industry leadership. By having a mandate to serve as a collaborative effort between government and industry on long range plans to sustain a domestic semiconductor capability, SEMATECH is widely credited with driving the technological innovations of that era by making strategic research investments and growing a workforce to support the industry. A similar whole-of-nation strategy is needed today to ensure that the country's economic and national security needs are met.

To maintain America's current innovation trajectory and win the race for global leadership in the technologies of the future, the United States must continue to lead the world in semiconductor innovation. In addition to the core recommendations pertaining to the U.S. Strategy on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem, the Senior Advisor should consider the following recommendations that are specific to the semiconductor industry.

Research and Development

- The NSTAC recommends the U.S. Government increase funding to federal scientific agencies for semiconductor research. Government funds should be directed towards basic research that seeks long-range, fundamental technology breakthroughs.

- The NSTAC highlights the success of the Electronics Resurgence Initiative under the Defense Advanced Research Projects Agency, discussed earlier in this report. The NSTAC recommends increased funding for ERI and further recommends that the Senior Advisor use this program as a model for other public private partnerships that support innovation in NS/EP technologies.

Workforce Development

- The Strategy should include a comprehensive, long-term plan to expose, attract, and recruit students at all levels, particularly women and minorities, to fields of study in science, technology, engineering, and math (STEM), internships, and advanced manufacturing programs.

- This plan should include significantly increased investment in STEM programs within the U.S. educational system.

Open Markets

- The Senior Advisor should work with other relevant U.S. agencies to ensure that U.S. semiconductor manufacturers have access to global markets for raw materials and essential components not made in the United States. While the majority of semiconductor research and development (R&D) and Intellectual Property (IP) creation occurs on U.S. soil, the supply chains for sourcing materials critical to the manufacturing process are global. The U.S. Government should work with its allies and like-minded countries to promote trade policies that ensure fair competition and access to raw materials, components, and human capital.

IP Protection

- The Senior Advisor and the Strategy should devote attention to the threat of IP theft aimed at the semiconductor industry. IP is the essence of the semiconductor industry and enforcing IP rights is essential to the industry's global competitiveness. The industry's high level of investment in R&D results in valuable IP (patents, trade secrets, source code, etc.), and its protection is critical to the industry's competitive position in the world.

APPENDIX C: STANDARDS BODIES

Standards bodies abound and are vital to promoting interoperability that enables competition and innovation to thrive across borders. There are several standards bodies that have enhanced technology choice and resiliency.

- Third Generation Partnership Project (3GPP) has been leading the development of global standards for 5G through releases that define technical specifications. Release 15 for fifth generation (5G) is complete and being used for 5G networks running on 4G network cores, and release 16 is underway. Content for release 17 has started as well and should be the final release for 5G as 6G content is currently being defined. 3GPP standards are later incorporated in standardization processes of the International Telecommunication Union.

- The Alliance for Telecommunications Industry Solutions, the North American partner of 3GPP, is focusing on technical aspects of a wide range of innovative ICT: 5G, unmanned aerial and connected vehicles, AI, distributed ledger (blockchain) technologies, cybersecurity, and identity management.

- The Institute of Electrical and Electronics Engineers Standards Organization is a longtime developer of standards development for AI. The March 2019 publication of *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* culminated a three-year process of global input and will provide guidance for standards.

- The Internet Engineering Task Force (IETF) defines internet technologies, including HTTP/3, being used as signaling in 5G and beyond. HTTP/3 is a crucial technology in 5G, as it is the protocol used by network functions to communicate with one another using JavaScript Object Notation for instructions. The IETF is also developing the virtualization specifications for 5G, including things like service function chaining that links virtualized functions such as radio access network base stations and packet core functions.

- The International Standardization Organization has developed a family of more than 12 standards on information and security management, which are used widely around the world.

- Trade groups, such as Groupe Speciale Mobile Association and Cellular Telecommunications Industry Association, facilitate collaboration, promote technical standards, and interoperability.

- Underwriters Laboratories (UL)[1] has offered standards for decades that promote interoperability, safety, and security through certification. UL 2900 series has started to address software assurance and cybersecurity of medical devices and industrial control systems.

[1] Underwriters Laboratories, "Cybersecurity Assurance and Compliance," https://www.ul.com/offerings/cybersecurity-assurance-and-compliance.

- Companies themselves are developing standards and approaches on their own and in collaboration with others. International Computer Security Association Labs, an independent division of Verizon, is looking at internet of things (IoT) Security Testing Framework[2] and Symantec offered an IoT Reference Architecture White Paper.[3] Several companies have developed technical and ethical standards for artificial intelligence, as exemplified by filings from AT&T, Google, and Microsoft in a recent National Institute of Standards and Technology consultation.

- There are a number of other standards that are being used for 5G, such as cloud technology standards and virtualization standards. They are not directly associated with 5G, but they define the technologies upon which 5G relies.

[2] *ISCA Labs,* "Internet of Things (IoT) Security Testing Framework," https://www.icsalabs.com/sites/default/files/body_images/ICSALABS_IoT_reqts_framework_v2.0_161026.pdf.

[3] Symantec, "An Internet of Things Reference Architecture," https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf.

SUBCOMMITTEE MEMBERS

Mr. David DeWalt, NightDragon Security and Subcommittee Chair

Ms. Katherine Gronberg, Forescout Technologies, Inc. and Working Group Co-Lead
Mr. Dean Hullings, Forescout Technologies, Inc. and Working Group Co-Lead

Name	Company
Mr. Larry Abram	AT&T, Inc.
Mr. Andrew Bonillo	Ciena Corp.
Mr. Christopher Boyer	AT&T, Inc.
Ms. Cherilyn Caddy	National Security Agency
Mr. James Carnes	Ciena Corp.
Ms. Kathryn Condello	CenturyLink, Inc.
Ms. Amanda Craig-Deckard	Microsoft Corp.
Mr. Michael Daly	Raytheon Co.
Mr. Donald Davidson	Synopsys, Inc.
Mr. James Diffell	Office of the Director of National Intelligence
Ms. Karen Evans	Department of Energy
Mr. Trey Herr	Microsoft Corp.
Mr. Rodney Joffe	Neustar, Inc.
Mr. Timothy Kocher	Department of Energy
Mr. Kent Landfield	McAfee, Inc.
Mr. Vico Loquercio	Avaya, Inc.
Mr. Peter Lord	Oracle Corp.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. John Neal	Symantec Corp.
Ms. Anita Patankar-Stoll	National Security Council
Mr. Thomas Patterson	Unisys, Inc.
Mr. Jon Peterson	Neustar, Inc.
Mr. Travis Russell	Oracle, Inc.

Mr. Jerry Scarborough	Raytheon Co.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Thomas Vincent	Verizon, Inc.
Mr. Milan Vlajnic	Communication Technologies, Inc.
Mr. Michael Woods	Verizon, Inc.

BRIEFERS – SUBJECT MATTER EXPERTS

Ms. Barbara Baffer	Ericsson
Ms. Jennifer Bisceglie	Interos
Mr. Jason Boswell	Ericsson
Mr. James Boyens	National Institute of Standards and Technology
Mr. Jeffrey Bratcher	FirstNet
Mr. Robert Bresne	Gartner, Inc.
Mr. Mark Chandler	Cisco
Dr. William Chappell	Defense Advanced Research Projects Agency
Mr. James Connell	JP Morgan Chase
Ms. Edna Conway	Cisco
Mr. Michael Daniel	Cyber Threat Alliance
Mr. Donald Davidson	Department of Defense
Mr. Andrew Dugan	CenturyLink
Mr. Benjamin Flatgard	JP Morgan Chase
Mr. James Goodrich	Semiconductor Industry Association
Mr. Thilo Hanemann	Rhodium Group
Mr. Mance Harmon	Hedera Hashgraph, LLC
Ms. Elsa Kania	Center for a New American Security
Mr. Richard Ledgett	MITRE
Dr. James Lewis	Center for Strategic and International Studies
Mr. Emile Monette	Synopsys, Inc.

Mr. Drew Morin	T-Mobile
Mr. Richard Reed	FirstNet
Ms. Evelyn Remaley	National Telecommunications and Information Administration
Ms. Diane Rinaldo	National Telecommunications and Information Administration
Mr. Daniel Rosen	Rhodium Group
Mr. Travis Russell	Oracle
Ms. Lynn Starr	Ericsson
Mr. Steve Stone	FireEye
Mr. Thomas Swanabori	Cellular Telecommunications Industry Association
Lt. Gen. Christopher Weggeman	United States Air Force
Mr. Eric Wenger	Cisco

SUBCOMMITTEE MANAGEMENT

Ms. Helen Jackson	President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO)
Ms. Sandra Benevides	NSTAC Alternate DFO
Ms. DeShelle Cleghorn	NSTAC Alternate DFO
Ms. Kayla Lord	NSTAC Alternate DFO
Ms. Laura Creel	Insight Technology Solutions, Inc.
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Barry Skidmore	Insight Technology Solutions, Inc.

APPENDIX E: ACRONYMS

3GPP	Third Generation Partnership Project
5G	Fifth Generation
AI	Artificial Intelligence
APL	Approved Products List
APT	Advanced Persistent Threat
BIS	Bureau of Industry and Security
CISA	Cybersecurity and Infrastructure Security Agency
COI	Community of Interest
CSIS	Center for Strategic and International Studies
CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
D/A	Department and Agency
DOC	Department of Commerce
DOD	Department of Defense
DODIN	Department of Defense Information Network
DOE	Department of Energy
ECRA	Export Control Reform Act
eNodeBs/eNB	Evolved Node B
EO	Executive Order
ESF	Enduring Security Framework
FCC	Federal Communications Commission
FIRRMA	Foreign Investment Risk Review Modernization Act of 2018
IC	Intelligence Community

ICT	Information and Communication Technology
IP	Intellectual Property
IT	Information Technology
IoT	Internet of Things
IQT	In-Q-Tel
ML	Machine Learning
NCF	National Critical Functions
NEC	National Economic Council
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NSC	National Security Council
NS/EP	National Security/Emergency Preparedness
NSF	National Science Foundation
NSIC	National Supply Chain Intelligence Center
NSTAC	National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
ONAP	Open Network Automation Platform
O-RAN	Open Radio Access Network
OSTP	Office of Science and Technology Policy
OTA	Other Transaction Authority
PPP	Public Private Partnership
QIS	Quantum Information Science
RAN	Radio Access Network
R&D	Research and Development

SDN	Software-Defined Networking
SDO	Standards Developments Organizations
SEMATECH	Semiconductor Manufacturing Technology Consortium
STEM	Science, Technology, Engineering, and Math
TSG	Technical Specifications Group
UL	Underwriters Laboratory

APPENDIX F: GLOSSARY

5G: A future, fifth generation mobile network, whose specification the ITU has not fully defined. It is expected to support 10 gigabits per second data rates and higher. Commercial 5G deployments are not expected until around 2020. (Newton's Telecom Dictionary)

Advanced Persistent Threat (APT): An adversary that possesses sophisticated levels of expertise and significant resources allowing it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of extracting information, undermining or impeding critical aspects of a mission, program, or organization, or positioning itself to carry out these objectives in the future. The APT: (1) pursues its objectives repeatedly over an extended period of time; (2) adapts to defenders' efforts to resist it; and (3) is determined to maintain the level of interaction needed to execute its objectives. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39)

Adversary: Any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (NIST SP 800-30)

Agency: Any executive department, military department, government corporation, government-controlled corporation, other establishment in the Executive Branch of the Government (including the Executive Office of the President), or any independent regulatory agency. Does not include: (1) the Government Accountability Office; (2) the Federal Election Commission; (3) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (4) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. (NIST Glossary of Information Security Terms – FIPS 200; 44 U.S.C., Sec. 3502)

Artificial Intelligence: The intelligence exhibited by machines or software. A term popularized by Alan Turing, it historically describes a machine that could trick people into thinking it was a human being via the Turing Test. Recently, scientists within this field largely have abandoned this goal to focus on the uniqueness of machine intelligence and learn to work with it in intelligent, useful ways. (Newton's Telecom Dictionary)

Availability: Ensuring timely and reliable access to and use of information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Communications: Modern network is the totality of users, devices, data, and applications. (The President's National Security Telecommunications Advisory Committee (NSTAC) Secure Government Communications (SGC) Subcommittee Definition)

Community of Interest: A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes and who must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains. (NIST Glossary of Information Security Terms – Committee on National Security Systems Instruction (CNSSI) 4009)

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructure can be owned and operated by both the public and private sector. (*Critical Infrastructure Protection Act of 2001,* 42 U.S.C.519c (e)) (NIST Glossary of Information Security Terms – CNSSI 4009, Adapted)

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. (NIST Glossary of Information Security Terms – CNSSI 4009)

Defense Industrial Base: The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. (Cybersecurity and Infrastructure Security Agency, "Defense Industrial Base Sector," https://www.dhs.gov/cisa/defense-industrial-base-sector)

Emerging Technologies: New, evolving, or innovative technologies. (NSTAC SGC Subcommittee Definition)

Enduring Security Framework: A cross-sector working group within the Critical Infrastructure Partnership Advisory Council, which was established by the Department of Homeland Security to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators. (Department of Homeland Security)

ICT Supply Chain Risk Management: The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. (NIST SP 800-161)

Information Technology: Equipment, processes, procedures, and systems used to provide and support information systems (computerized and manual) within an organization and those reaching out to customers and suppliers. (Newton's Telecom Dictionary)

Intelligence Community: The Intelligence Community's mission is to collect, analyze, and deliver foreign intelligence and counterintelligence information to America's leaders so they can make sound decisions to protect the United States. (https://www.intelligence.gov/)

International Computer Security Association (ICSA) Labs: ICSA Labs, an independent division of Verizon, has been providing credible, independent, third-party product assurance for end-users and enterprise since 1989. ISCA Labs provides third-party testing and certification of security and health IT producers, as well as network-connected devices, to measure product compliance, reliability, and performance for most of the world's top technology vendors. (ISCA Labs, https://www.icsalabs.com/)

Internet of Things: The *Internet of Things* (IoT) consists of networks of sensors attached to objects and communications devices, providing data that can be analyzed and used to initiate automated actions. The attributes of this world of things may be characterized by low energy consumption, auto-configuration, embeddable objects, etc. The data also generates vital intelligence for planning, management, policy, and decision making. (Cisco, https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-57/153-internet.html)

Internet Protocol: Part of the Transmission Control Protocol/IP family of protocols describing software that tracks the internet address of nodes, routes outgoing messages, and recognizes incoming messages; also used in gateways to connect networks at open systems interconnection network level 3 and above. (Newton's Telecom Dictionary)

Interoperability: The ability of independent systems to exchange meaningful information and initiate actions from each other in order to operate together for mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility for use in services outside the direct control of the issuing assigner. (International Organization for Standardization Technical Committee 46/Subcommittee 9)

Information Sharing and Analysis Center (ISAC): Trusted entities established by critical infrastructure key resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government. ISACs take an all-hazards approach and have strong reach into their respective sectors, with many reaching over 90 percent penetration. Services provided by ISACs include risk mitigation, incident response, and alert and information sharing. (National Council of ISACs, http://www.isaccouncil.org/aboutus.html)

International Telecommunication Union (ITU): ITU is the United Nations specialized agency for information and communication technologies – ICTs. Founded in 1865 to facilitate international connectivity in communications networks, ITU allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect and strive to improve access to ICTs to underserved communities worldwide. (ITU, https://www.itu.int/en/Pages/default.aspx)

Lowest Price Technically Acceptable (LPTA): A source selection process that is appropriate when best value is expected from selecting the technically acceptable proposal with the lowest price. The following factors apply when using LPTA: (1) Evaluation factors and significant subfactors that establish the requirements of acceptability shall be set forth in the solicitation, and (2) Tradeoffs are not permitted. (Defense Acquisition University).

Machine Learning: A type of AI in which computers use huge amounts of data to learn how to do tasks rather than being programmed to do them. (Oxford Learner's Dictionary)

Material Science: The scientific study of the properties and applications of materials of construction or manufacture, such as ceramics, metals, polymers, and composites. (Merriam-Webster's Dictionary)

National Security/Emergency Preparedness (NS/EP) Communications: Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States (47 Code of Federal Regulations Chapter II, § 201.2(g)). NS/EP communications include primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international), to include communicating with itself; the Legislative and Judicial branches; state, territorial, tribal, and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications further include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee based on Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012])

Networks: Information system(s) implemented with a collection of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary of Information Security Terms – NIST Interagency Report (NISTIR) 7298 – Revision 2)

Protocol: A set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (NIST Glossary of Information Security Terms – NISTIR 7298 – Revision 2)

Quantum Computing: A developing computing technology that exploits the properties of atoms to create a radically different type of computer architecture through quantum physics. Quantum computing relies on the basic traits of an atom, such as the direction of its spin (left-to-right, right-to-left) to create a state, such as "1" or "0", as much as conventional computers use variations in electrical energy (positive and negative polarity). (Newton's Telecom Dictionary)

Radio Access Network: Controls the transmission and reception of radio signals across cellular networks.

Reliability: A measure of how dependable a system is once you use it. (Newton's Telecom Dictionary)

Resilience: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (Presidential Policy Directive-8: National Preparedness)

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Security: A way of insuring data on a network is protected from unauthorized use. Network security measures can be software-based where passwords restrict users' access to certain data files or directories. This kind of security is usually implemented by the network operating system. Audit trails are another software-based security measure, where an ongoing journal of what users did what with what files is maintained. Security can also be hardware-based, using more traditional lock and key. (Newton's Telecom Dictionary)

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-53, CNSSI 4009, Adapted)

Trustworthiness: The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (NIST SP 800-39, CNSSI-4009)

World Trade Organization: The World Trade Organization (WTO) is the only global international organization dealing with the rules of trade between nations. At its heart are the WTO agreements, negotiated and signed by the bulk of the world's trading nations and ratified in their parliaments. The goal is to ensure that trade flows as smoothly, predictably and freely as possible. (World Trade Organization)

APPENDIX G: BIBLIOGRAPHY

Accenture. "New Research from Accenture Strategy highlights Economic and Societal Impact of Investing in 5G Infrastructure," January 12, 2017. Last Accessed July 24, 2019. https://newsroom.accenture.com/news/new-research-from-accenture-strategy-highlights-economic-and-societal-impact-of-investing-in-5g-infrastructure.htm.

"A First Step in Securing the Global Technology Supply Chain: Introducing The Open Group Trusted Technology Provider Framework Whitepaper," *The Open Group Blog*, February 9, 2011. https://blog.opengroup.org/2011/02/09/a-first-step-in-securing-the-global-technology-supply-chain-introducing-the-open-group-trusted-technology-provider-framework-whitepaper/.

AT&T Developer Program. "Long Term Evolution (LTE)." Last Accessed July 9, 2019. https://developer.att.com/technical-library/network-technologies/long-term-evolution.

Baffer, Barbara, Boswell, Jason, and Starr, Lynn. "Supplier Perspective on 5G Risks and Supply Chain." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 25, 2019.

Bisceglie, Jennifer and Brese, Robert. "Manage Supply Chain Risk with Facts…Not Opinion." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, October 30, 2018.

Boyens, Jon M. "Cyber Supply Chain Risk Management." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, November 1, 2018.

Bratcher, Jeffrey and Reed, Richard. "First Responder Network Authority." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, November 8, 2018.

Budget and Spending. "Executive Order on Ensuring Transparency, Accountability, and Efficiency in Taxpayer Funded Union Time Use," White House, Issued May 25, 2018. https://www.whitehouse.gov/presidential-actions/executive-order-ensuring-transparency-accountability-efficiency-taxpayer-funded-union-time-use/.

Bundeministerium der Verteidigung. "Entwicklung des Organisationsbereichs bei der Bundeswehr." Last Accessed July 5, 2019. https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw.

Canada. Parliament. House of Commons. "*An Act Respecting National Security Matters,"* Forty-Second Parliament, First sess. Bill C-59. Ottawa: Parl.CA, 2019. Last Accessed July 3, 2019. https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading.

Chandler, Mark and Wenger, Eric. "5G Standards Setting." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 25, 2019.

Chappell, Dr. William and Duane-Chambers, Richard. "DARPA Perspective on 5G and National Security." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, May 23, 2019.

Chatzky, Andrew and McBride, James. "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, Last Updated May 13, 2019. Last Accessed July 3, 2019. https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

Common Public Radio Interface. "Industry Leaders Releasing the New eCPRI Specification for 5G – eCPRI V 2.0 with Additional Functionality for Interworking," May 10, 2019. Last Accessed July 9, 2019. http://www.cpri.info/press.html.

Connell, James M. and Flatgard, Benjamin W. "Finance Sector-wide Methodology for Security Evaluation." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, December 4, 2018.

Conway, Edna. "The Security of Critical Components to the Nation's Telecommunications Infrastructure." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, October 25, 2018.

Cybersecurity and Infrastructure Security Agency (CISA). "National Critical Functions Set," Department of Homeland Security. Last Accessed July 3, 2019. https://www.dhs.gov/cisa/national-critical-functions-set.

Cybersecurity and Infrastructure Security Agency (CISA). "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," Department of Homeland Security. Last Accessed July 3, 2019. https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

Daniel, Michael. "National Cybersecurity Strategy and Policy." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, May 2, 2019.

Davidson, Donald. "Cyber-SCRM and 'Commercially Acceptable Global Sourcing Standards'." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, January 31, 2019.

DeWalt, David. NSTAC Member and Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Subcommittee Chair Comments During the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019.

Defense Advanced Research Projects Agency. "DARPA Electronics Resurgence Initiative," Last Updated June 20, 2019. Last Accessed July 3, 2019. https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.

Defense Acquisition University. "Lowest Price Technically Acceptable." Last Accessed July 12, 2019. https://www.dau.mil/acquipedia/pages/articledetails.aspx#!484.

Department of Defense. "Summary of the 2018 DOD Artificial Intelligence Strategy-Harnessing AI to Advance our Security and Prosperity." Last Accessed July 3, 2019. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

Department of Homeland Security. "Enduring Security Framework." https://www.dhs.gov/keywords/enduring-security-framework.

Donahue, Thomas. "The Asymmetric Era as a Driving Need for a New Security Economic Strategy." Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019.

Dugan, Andrew. "Assuring the Next Generation Core." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, November 5, 2018.

État-major des armées. "La Cyberdéfense au Cœur des Opérations," January 24, 2018. Last Accessed July 5, 2019. https://www.defense.gouv.fr/ema/transformation/actualites/la-cyberdefense-au-coeur-des-operations

Executive Office of the President. "Memorandum for the Heads of Executive Departments and Agencies-FY 2020 Administration Research and Development Budget Priorities," Published July 31, 2018. Last Accessed July 3, 2019. https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf.

Federal Bureau of Investigation. "Chinese Hackers Indicted," December 20, 2018. Last Accessed July 8, 2019. https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

Federal Communications Commission, Communications Security, Reliability and Interoperability Council, Working Group 3. "Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks," September 2018. Last Accessed July 24, 2019. www.fcc.gov/files/csric6wg3sept18report5gdocx-0.

Communications Security, Reliability and Interoperability Council. "Communications Security, Reliability and Interoperability Council," Federal Communications Commission. Last Accessed July 3, 2019. https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

Foster, Tom. "What Happens When A Wildly Ambitious Young Startup Decides to Work With the Military?" *Inc. Magazine,* June 2019.

Goodrich, James. "Long Range ICT Industry Strategy." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, May 2, 2019.

Government of the Czech Republic. "Prague 5G Security Conference Announces Series of Recommendations: The Prague Proposals," March 5, 2019. Last Accessed July 3, 2019. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Hanemann, Thilo and Rosen, Daniel. "China in the ICT Ecosystem." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 12, 2019.

Hardesty, Linda. "Cisco's Early Bet on RAN Virtualization Propels Altiostar," *FierceWireless,* May 19, 2019. Last Accessed July 9, 2019. https://www.fiercewireless.com/tech/cisco-s-early-bet-ran-virtualization-propels-altiostar.

Hardesty, Linda. "O-RAN Aims to Eliminate Vendor Lock-in at the Radio Access Network," *FierceWireless,* March 19, 2019. Last Accessed July 9, 2019. https://www.fiercewireless.com/wireless/o-ran-aims-to-eliminate-vendor-lock-at-radio-access-network.

Harmon, Mance. "Distributed Ledger Technology for Security and Recovery." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 28, 2019.

Hunt, Galen. "Securing the Billions of Devices Around Us." Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019.

House Committee on the Budget, "Budget Functions." Last Accessed July 3, 2019. https://budget.house.gov/budgets/budget-functions.

ICSA Labs. "Internet of Things (IoT) Security Testing Framework," Oct. 26, 2016. https://www.icsalabs.com/sites/default/files/body_images/ICSALABS_IoT_reqts_framework_v2.0_161026.pdf.

Infrastructure and Technology. "America Will Dominate the Industries of the Future," White House, Issued on February 7, 2019. Last Accessed July 3, 2019. https://www.whitehouse.gov/briefings-statements/america-will-dominate-industries-future/.

Infrastructure and Technology. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, Issued May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

In-Q-Tel. "Our History." Last Accessed July 3, 2019. https://www.iqt.org/our-history/.

Kania, Elsa. "China's AI Strategy." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 18, 2019.

Kania, Elsa. "China's Quantum Future," *Foreign Affairs,* September 26, 2018. Last Accessed July 3, 2019. https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future.

Kahn, Michael and Lopatka, Jan. "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence," *Reuters,* May 3, 2019. Last Accessed July 3, 2019. https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2.

Kramer, Franklin D. "Achieving International Cyber Stability," *Atlantic Council,* September 2012. Last Accessed July 3, 2019. https://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf.

Krebs, Christopher. Comments During the Joint NIAC NSTAC Meeting, Redmond, WA, June 13, 2019.

Ledgett, Rick. "Technology Challenges." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 26, 2019.

Lewis, James. "How Will 5G Shape Innovation and Security: A Primer," Center for Strategic and International Studies, December 6, 2018. Last Accessed July 10, 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdfCite.

Lewis, James. "U.S. Foreign Policy and National Security and Emergency Preparedness Technology Issues." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, May 9, 2019.

Linux Foundation Projects. "Open Network Automation Platform." Last Accessed July 24, 2019. https://www.onap.org/about.

Manuel, Kate M., et al. "Domestic Content Restrictions: The Buy American Act and Complementary Provisions of Federal Law," *Congressional Research Service,* September 12, 2016. Last Accessed July 3, 2019. https://fas.org/sgp/crs/misc/R43354.pdf.

Ministère Des Armées. "PROJET DE LOI DE PROGRAMMATION MILITAIRE." Last Accessed July 15, 2019. https://www.defense.gouv.fr/content/download/523150/8769279/file/LPM%202019-2025%20-%20Rapport%20annex%C3%A9.pdf.

Monette, Emile. "Current DHS ICT Supply Chain Efforts." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 21, 2019.

Morine, Drew. "ICT Supply Chain Task Force Threat Criteria Working Group Lead." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 16, 2019.

Morris, Iain. "Huawei Dwarfs Ericsson, Nokia on R&D Spend in 2017," *LightReading*, April 3, 2018. Last Accessed July 24, 2019. https://www.lightreading.com/artificial-intelligence-machine-learning/huawei-dwarfs-ericsson-nokia-on-randd-spend-in-2017/d/d-id/741944.

Morris, Iain. "The Future's Bright, the Future's ORAN," *LightReading*, June 28, 2018. Last Accessed July 3, 2019. https://www.lightreading.com/mobile/fronthaul-c-ran/the-futures-bright-the-futures-oran/d/d-id/744294.

National Cyber Security Center. "About the NCSC." Last Accessed July 3, 2019. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

National Infrastructure Advisory Council. "National Infrastructure Advisory Council," Department of Homeland Security. Last Accessed July 9, 2019. https://www.dhs.gov/national-infrastructure-advisory-council#.

National Security Telecommunications Advisory Committee. *NSTAC Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*, Washington, DC: NSTAC, April 2, 2019. https://www.dhs.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem.pdf.

National Security Telecommunications Advisory Committee. *NSTAC Report to the President on a Cybersecurity Moonshot*, Washington, DC: NSTAC, November 14, 2018. https://www.dhs.gov/sites/default/files/publications/DRAFT_NSTAC_ReportToThePresidentOnACybersecurityMoonshot_508c.pdf.

Office of the Secretary. "Loaned Executive Program," Department of Homeland Security. Last Accessed July 3, 2019. https://www.dhs.gov/loaned-executive-program.

Office of the United States Trade Representative. "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," Executive Office of the President, March 22, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

Quora. "Why Bell Labs Was So Important To Innovation In The 20th Century," *Forbes*, July 19, 2017. Last Accessed July 3, 2019. https://www.forbes.com/sites/quora/2017/07/19/why-bell-labs-was-so-important-to-innovation-in-the-20th-century/#5e568db7015f.

Remaley, Evelyn and Rinaldo, Diane. "5G Market Dependencies and Complexities." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, March 26, 2019.

Russell, Travis. "5G Ecosystem - The Architecture and the Vendors." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, November 8, 2018.

SDxCentral. "What is Edge Computing?" Last Accessed July 24, 2019. https://www.sdxcentral.com/edge/definitions/what-multi-access-edge-computing-mec/.

Stone, Steve. "ICT Intrusion Takeaways." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, November 8, 2018.

Swanabori, Thomas. "Spectrum, 5G networks, and Cybersecurity." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, April 18, 2019.

Symantec, "*An Internet of Things Reference Architecture*," *Symantec*, 2016. Last Accessed July 5, 2019. https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf.

Thomas, Christopher. "A New World Under Construction: China and Semiconductors," *McKinsey*, November 2015. Last Accessed July 10, 2019. https://www.mckinsey.com/featured-insights/asia-pacific/a-new-world-under-construction-china-and-semiconductors.

Underwriters Laboratories. "Cybersecurity Assurance and Compliance." Last Accessed July 17, 2019. https://www.ul.com/offerings/cybersecurity-assurance-and-compliance.

United States. Cong. House. "*Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act,"* 115th Cong., 2nd sess. HR 7327. Washington: Congress.gov, 2018. Last Accessed July 3, 2019. https://www.congress.gov/bill/115th-congress/house-bill/7327/text.

United States. Cong. House. "*John S. McCain National Defense Authorization Act for Fiscal Year 2019,"* 115th Cong. HR 5515. Washington: Congress.gov, 2019. Last Accessed July 3, 2019. https://www.congress.gov/bill/115th-congress/house-bill/5515.

Weggeman, Lt. Gen. Chris. "DOD Perspective on 5G and China." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Advancing Resiliency and Fostering Innovation in the ICT Subcommittee, Arlington, VA, May 16, 2019.

White House. "National Cyber Strategy of the United States of American," September 2018. Last Accessed July 8, 2019. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.