THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

DRAFT NSTAC REPORT TO THE PRESIDENT

on Communications Resiliency

TBD

Table of Contents

List of Figures

Executive Summary

Nearly a decade has passed since the President's National Security Telecommunications Advisory Committee (NSTAC) last reviewed the Nation's communications resiliency posture. In its 2011 *NSTAC Report to the President on Communications Resiliency* (Communications Resiliency Report),[1] the committee examined the then-current communications resiliency landscape and provided recommendations to the U.S. Government on how to enhance the survivability and availability of networks. Recent wide-scale emergencies, like the coronavirus (COVID-19) pandemic, extreme natural disasters, and broadly impactful security events, demonstrate the need to reexamine the resiliency and national security and emergency preparedness (NS/EP) of the Nation's communications networks.

In May 2020, the Executive Office of the President tasked NSTAC with examining the resilience of the Nation's communications infrastructure to better understand and address these challenges moving forward. In response, NSTAC established the Communications Resiliency Subcommittee in June 2020 with two distinct phases and areas of focus.

In phase I, NSTAC conducted an immediate-term examination of the resiliency of the Nation's information and communications technology (ICT) ecosystem during COVID-19. The committee concluded phase I in October 2020 with the *NSTAC Letter to the President on Communications Resiliency*,[2] which provided a series of actionable recommendations to assist the Administration with its ongoing policy response to the pandemic.

During phase II, NSTAC conducted a broader, forward-looking examination of the resilience of the Nation's NS/EP communications posture. Leveraging its 2011 Communications Resiliency Report and its recent work on emerging technologies (e.g., software-defined networking, network functions virtualization, 5G networks), NSTAC conducted a strategic assessment of potential future NS/EP communications resiliency challenges. This assessment: (1) outlines the general state of the ICT ecosystem 8 to 10 years in the future; and (2) examines how future networks, services, and related infrastructure could assure the necessary level of security and resilience in a variety of event scenarios.

The focus of this report has shifted since the original tasking in May 2020. While the report outlines some of the challenges the Nation faces, it highlights the evolution of the ICT ecosystem toward a highly resilient environment of federated, hyperconnected, distributed networks managed via software. With the advent of 5G and other network advances, the Nation now stands at a point where not only can the ICT providers create meshed and highly resilient operating environments, but enterprises (both Government and commercial) can avail themselves of these capabilities as well. NSTAC contends the resiliency benefits of new technologies and innovations referenced in this report and supported by expert briefings throughout the study period will position the Nation's economy to not only derive cost and operational efficiencies, but to create an environment for U.S. innovation and leadership in

[1]National Security and Telecommunications Advisory Committee, "NSTAC Report to the President on Communications Resiliency," April 2011, https://www.cisa.gov/publication/2011-nstac-publications

[2]National Security and Telecommunications Advisory Committee, "NSTAC Letter to the President on Communications Resiliency," October 2020, https://www.cisa.gov/publication/2020-nstac-publications

the global economy. As such, the recommendations in this report suggest actions the Administration can take to support the deployment, adoption, and mastery of these key technologies, putting the Nation in a better position to support the Nation's security, economic security, and emergency preparedness goals.

Introduction

A resilient communications network is critical to economic security, essential services, emergency response, and most facets of modern life. The concept of resilient networks dates back decades but can be defined as networks "with the ability to operate and maintain acceptable level of service under the presence of adverse conditions."[3] Paul Baran, working at RAND for the U.S. Air Force in the 1960s, conducted extensive research on the survivability of networks and

> "…In 1964, Paul Baran published On Distributed Communications, in which he critiqued then existing military communications design as a vulnerable, centralized telecommunications network. Diagrammed as a spoke model with a hub in the middle, an enemy could successfully take out a single point causing the network to fail. Baran advocated that the U.S. Department of Defense (DoD) redo their entire communications system, moving to a decentralized, packet switched design. In this network, diagramed as a mesh network, there is no central point of control and each node in the network is served by redundant links. Data, transmitted over shared communications lines, would be in individually addressed packets, where nodes in the network would read the addresses and forward their packets to its destination along the known available route. This network would have redundancy and ability to route around failure. Baran wrote, 'We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built-even in the thermonuclear era.'"[4]

Since 1964, the Nation's telecommunications network has indeed transformed from a single-provider (AT&T) centralized network architecture to a global federation of highly distributed, interconnected networks accessed by end users via wired and wireless access providers. Each new modality of commercial access (such as commercial wireless and cable providers) has created its own "meshed" environments, leveraging the same principles initiated more than 50 years ago. This Internet Protocol (IP)-driven ecosystem is sometimes referred to as a system of systems, or, alternatively, a system of resilient systems.

This resilient foundation, augmented by affordable and ubiquitous mobile access, created an environment of extraordinary innovation. Fueled by big data, cloud computing, the Internet of Things (IoT), and ever higher levels of mobile traffic, this wave of innovation dramatically changed the traffic patterns of enterprises worldwide, which in turn contributed to further growth in the ICT ecosystem. While this traffic expansion was accompanied by greater performance, capacity, and processing speeds of networks, the dynamic traffic patterns associated with these innovations challenged traditional enterprise network architectures. As noted by William Stallings in Foundations of Modern Networking, some of the large scale changes driving traffic complexity included the network convergence of voice, data, and video traffic, which created unpredictable traffic patterns incorporating large multimedia data transfers, unified communications, and the heavy use of mobile devices.[5] These innovations impacted both network service providers as well as those managing enterprise architectures. William Stallings summarized the converging forces well: "Even with the greater capacity of transmission schemes and the greater performance of network devices, traditional network architectures are increasingly inadequate in the face of the growing complexity, variability, and high volume of the imposed load. In addition, as quality of service (QoS) and quality of experience (QoE) requirements imposed on the network are expanded because of the variety of applications, the traffic load must be handled in an increasingly sophisticated and agile fashion."[6]

[3]Mohammed, Abdul Jabbar, Hutchison, David, and Sterbenz, James, "Towards Quantifying Metrics for Resilient and Survivable Networks," https://resilinets.org/papers/Mohammad-Hutchison-Sterbenz-2006.pdf

[4]Baran, Paul, RAND, "On Distributed Communications," http://www.cybertelecom.org/notes/baran.htm

[5]Stallings, William, "Foundations of Modern Networking: SDN, NFV, QoE, IoT and Cloud," http://williamstallings.com/Network/

[6]Stallings, William, "Foundations of Modern Networking: SDN, NFV, QoE, IoT and Cloud," http://williamstallings.com/Network/

To address the challenges and new complexity of networks, management of all enterprise network architectures and commercial networks has undergone substantive change. Operations has transitioned from network functions implemented through dedicated devices (such as switches, routers, and application delivery controllers) to traffic and services managed via software-defined networking (SDN), network function virtualization (NFV), and well-defined Application Programming Interfaces (API).

SDN programmatically deconstructs control, data, and management plane traffic. The resulting changes allow equipment to (1) dynamically support fluctuating traffic volume and security requirements, (2) apply consistent policies (for example, access or security) across a broad array of network devices from a centralized control location, and (3) quickly scale capacity. SDN, NFV, and APIs, working independently and together, also provide a significant degree of vendor independence, allowing the network manager to add, drop, or change allocated resources, capabilities, and services in response to evolving business needs, security issues, or customer demands.

This move toward SDN/NFV has been happening at both the commercial network and enterprise levels, with each providing the impetus for further evolution. The large hyperscalers offering scalable cloud computing services, such as Microsoft, Google, and Amazon Web Services, were some of the early adopters of these technologies and have leveraged them to drive their business success. "When it was first deployed by large enterprises, such as Google and Amazon, SDN helped them create scalable data centers, facilitate network resources and new server expansion, and reduce the workload for IT administrators. SDN optimized the efficiency of the upscaling process for these large companies and quickly drew the attention of other large companies who swiftly adopted SDN to improve their upscaling efficiency."[7]

As this new Administration begins, the state of current distributed network architectures will expand and drive toward even more network densification, connections, capacity, and capability across varied network paths. This expansion will provide a resilient national communications infrastructure that can serve as a platform for innovation. These densified ICT platforms, whether provided by the transport, edge, or cloud environments coupled with cloud-native microservices at the enterprise level, present the opportunity to create an enterprise-specific distributed architecture on these cloud, edge, and access platforms being deployed today. It will thus be essential to build out the enterprise ICT space into a more resilient and innovation-friendly platform through which this country can retain leadership of the digital economy.

The resiliency benefits of the technologies referenced throughout this report position the Nation's economy to not only derive cost and operational efficiencies, but to create an environment for U.S. innovation and leadership in the global economy. Accomplishing these goals will require further deployment of ICT infrastructure to support wired and wireless densification, and continued adoption and subsequent mastery of these platforms and technologies by the Nation, resulting in a stronger, more secure, and more resilient economy. Recommendations in this report provide actions the Administration can take to support the deployment, adoption, and mastery of these technologies. The result will be an ICT ecosystem better positioned to support the Nation's security, economic security, and emergency preparedness goals.

Scoping and Charge

In May 2020, the Executive Office of the President tasked NSTAC with examining the resilience of the Nation's communications infrastructure to better understand and address challenges moving forward. In response, NSTAC established the Communications Resiliency Subcommittee in June 2020 with two distinct phases and areas of focus.

[7] IBM, "What is Software Defined Networking (SDN)?," https://www.ibm.com/services/network/sdn-versus-traditional-networking

In phase I, NSTAC conducted an immediate-term examination of the resiliency of the Nation's ICT ecosystem during COVID-19. The committee concluded phase I in October 2020 with the *NSTAC Letter to the President on Communications Resiliency*,[8] which provided a series of actionable recommendations to assist the Administration with its ongoing policy response to the pandemic.

During phase II, NSTAC conducted a broader, forward-looking examination of the resilience of the Nation's NS/EP communications posture over the next 8 to 10 years. Leveraging its 2011 Communications Resiliency Report and its recent work on emerging technologies (e.g., software-defined networking, network functions virtualization, 5G networks), NSTAC conducted a strategic assessment of potential NS/EP communications resiliency challenges. This assessment will: (1) outline the general state of the ICT ecosystem 8 to 10 years in the future and (2) examine how future networks, services, and related infrastructure could maintain the necessary level of security and resilience in a variety of scenarios.

Subcommittee Process

NSTAC used several research methods, including receiving subject matter expert (SME) briefings and reviewing reports and articles on communications resiliency. NSTAC heard from public sector, private sector, analysts, and academic experts on the resiliency of the ICT infrastructure, the survivability and reliability of networks, how COVID-19 impacted NS/EP communications, and where resiliency is needed to strengthen future NS/EP functions and the ICT ecosystem.

To this end, NSTAC:

- Conducted bi-weekly meetings with the subcommittee members;
- Received 27 briefings from SMEs;[9]
- Reviewed federal ICT policies, regulations, guidance, and reports; and
- Reviewed current industry best practices and relevant technology research.

Summary of Report Structure

This report is divided into the following areas:

1. **Introduction** – Provides background information on charter, phase I, and phase II goals and clarifies the importance of deployment, adoption, and mastery of key technologies over the next 8 to 10 years to maintain the security and resilience of network communications infrastructure.
2. **Future State of ICT** – Describes the expected growth and "wanted state" of key ICT segments, such as wireless, wireline, satellite, public safety, and power. Summarizes the evolution of network architectures and security capabilities that are expected throughout the same period. Section 2.2 further details how major technologies and resources will be leveraged to achieve the desired vision across ICT.
3. **Potential Resiliency Stressors on the Future Network** – Evaluates four scenarios at a high level to assess their impact on the future state of ICT infrastructure to inform further recommendations. These scenarios are 1) wide-scale Electromagnetic Pulse (EMP) disruptions and outages, (2) position, navigation, and timing (PNT) disruptions, (3) long-term outage (LTO) of electrical power, and (4) supply chain-based cyber-attack.
4. **Non-Dependent Challenges** – Highlights independent factors that could significantly impact the realization of the desired state of ICT in the future. These are broadly categorized as 1) technological threats 2) technological discoveries 3) global market destabilization.
5. **Summary of Findings and Analysis of the Future State of ICT** – This section provides an overview of foundational elements that must be in place in order to deliver the desired security and resilience outcomes in future communications networks. These findings are supported by repeated observation of recurring themes or precursors noted throughout briefings and study materials.

[8]National Security and Telecommunications Advisory Committee, "NSTAC Letter to the President on Communications Resiliency," October 2020, https://www.cisa.gov/publication/2020-nstac-publications

[9]Please refer to the Briefer List in Appendix A for the full list of briefers.

6. **Summary of Actions the Administration Can Take to Support Future ICT Vision** – NSTAC's recommendations are provided in four categories:

- Public/Private Planning, Consultation and Risk Assessments
- Recommendations to Support the Deployment of Future Networks
- Recommendations to Support the Adoption of Key Technologies
- Utilizing Testbeds to Enable Mastery of Quantum and AI Technologies

7. **Conclusion** – By adopting and mastering key technologies, NSTAC believes the Nation will be in a better position to support its national security, economic security, and emergency preparedness goals.

The Future State of ICT

Communications networks are more integrated into the economic, social, and national security fabric of the Nation than ever before. At the same time, communications systems and services are also more interconnected – even hyperconnected. This complex yet flexible mesh of networks, data, and services produces a resilient web of connectivity that offers unprecedented opportunities for enterprises and individuals to incorporate secure, resilient connections that leverage an ever-increasing array of devices, sensors, and applications harnessing data in new and innovative ways.

ICT Vision

As noted in the October 2020 *NSTAC Letter to the President on Communications Resiliency*,[10] the rapid adaptation and reconfiguration of network architecture in response to COVID-19-related traffic shifts demonstrated the flexibility and resilience of today's networks. Most providers saw significant increases in overall traffic and a far different pattern of high usage, particularly for residential customers working and learning from home. To rebalance traffic loads on networks, U.S. providers leveraged traffic engineering powered by software-defined networks, network function virtualization, artificial intelligence, and cloud and edge computing. Despite the challenges of these rapid shifts—occurring over just a few weeks in March 2020—most networks saw negligible adverse impacts.[11] Future advancements should make the immense network reconfiguration performed in weeks last year possible in a fraction of the time.

Today's rapid pace of technological innovation in communications technology shows no signs of slowing down. Hardware continues to evolve at a rapid pace and will become increasingly capable of harnessing new levels of processing speed, energy performance, and scale. Software-defined networking is transforming the way entities build and operate networks and deliver real-time services. Cloud and virtualization technologies will continue to ensure improved cost efficiency and adaptability, and Secure Development and Operations (DevOps) will speed up time to market. The integration of artificial intelligence (AI) into fully programmable networks promises to turn complexity into efficiency. Smaller, simpler, low-power devices will make it possible to embed connectivity everywhere. The emerging technology landscape will provide smart materials and alternative energy technologies to build sustainable, eco-friendly networks that are both higher performance and more energy efficient than today's networks. These innovations will deliver an ever-denser and ever-more-converged era of hyperconnectivity across all elements of the communications sector.

As networks increasingly become critical components of society, resilience and security capabilities are crucial. As noted previously, the network must be able to provide service under adverse conditions, such as when part of the infrastructure is disabled due to natural disasters, local disturbances, or breakdowns in society, and it must offer robust resistance against deliberate malicious attacks. Cloud-native microservices will enable a distributed core that brings various functions

[10]National Security and Telecommunications Advisory Committee, "NSTAC Letter to the President on Communications Resiliency," October 2020, https://www.cisa.gov/publication/2020-nstac-publications

[11]The Broadband Deployment Advisory Committee to the Federal Communications Commission, "Report and Recommendations: COVID-19 Response," October 29, 2020, https://www.fcc.gov/sites/default/files/bdac-disaster-response-recovery-_approved-rec-10292020.pdf

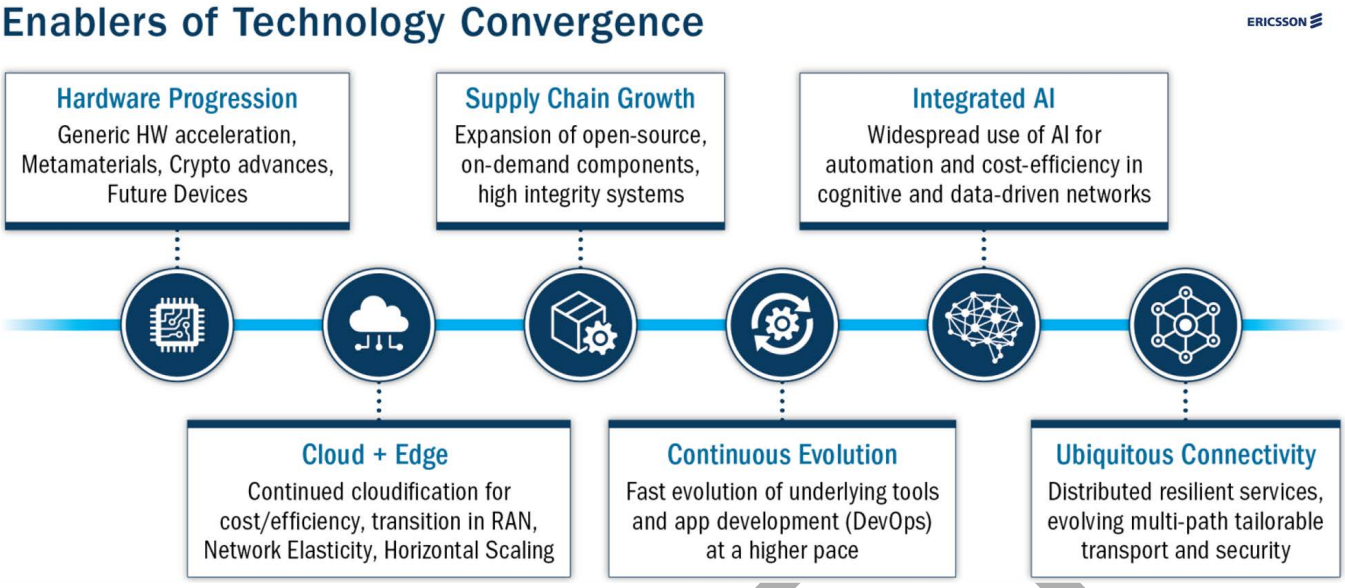

Figure 1. Enablers of Technology Convergence[12]

closer to the network edge to provide faster responses (lower latency), improved network resiliency, and network segmentation for isolation of cyberattacks.

To power the full use of digitalization and automation for society, future networks need high-precision location positioning and detailed sensing capabilities from their surroundings. These networks must also leverage advanced AI, automation, and orchestration capabilities to enable cognitive networks that will continuously self-learn at scale through experiences with and observations of the network environment. These advancements will combine ubiquitous connectivity with densification to achieve extreme coverage, faster computing with network distribution to achieve lower latencies and greater resiliency, and finer control with functional disaggregation to automatically make precise real-time decisions. Real time monitoring and measurement will evolve from traditional network-focused key performance indicators to user experience-focused key quality indicators (KQI) with zero-touch management to enable rapid service adaptability and greater network resiliency.

Wireline Segment

The wireline segment continually evolves to meet the demands of enterprises and consumers while providing backhaul transport back to core services and connectivity to other communications segments, including wireless, satellite, and broadcast. As customers demand higher bandwidth and lower latency, wireline infrastructure continues to transition away from legacy copper toward fiber optic connectivity; nearly all businesses and many homes are expected to have fiber optic connectivity by 2030.[13,14]

Wireline fiber growth enables—and is driven by—wireless technologies. 5G cellular, specified by 3GPP, and Wi-Fi 6, specified by IEEE, with their follow-on technologies, will enable exponentially more devices and sensors to connect to networks, and a robust wireline backbone will be vital in handling the backhaul for these new connections. The growth and evolution of connected IoT devices, and particularly of autonomous devices, will drive demand for increasingly lower latency of connectivity and compute resources. This demand is already driving growth of "edge computing" to meet latency demands while maintaining economies of scale

[12]Graphic adapted from: Tatipamula, Mallik and Ekudden, Erik, Ericsson, "Future Technology Trends and Ericsson's Outlook Towards 6G" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 10, 2020)

[13]Cyphers, Bennet, Electronic Frontier Foundation, "The Case for Fiber to the Home, Today: Why Fiber is a Superior Medium for 21st Century Broadband," October 16, 2019, https://www.eff.org/wp/case-fiber-home-today-why-fiber-superior-medium-21st-century-broadband

[14]Dugan, Andrew, Lumen Technologies, "The Future of Networking" (Briefing to the NSTAC CR Subcommittee. Arlington, VA, December 1 and 10, 2020)x

and access to the robust data and analytic power necessary to power AI enabled autonomous machines.

Wireline networks will continue to flatten, with more interconnection and meshing driving increased resiliency and flexibility, particularly when paired with AI-powered SDN and NFV. As networks continue to evolve, the low-latency, high-bandwidth connectivity of people, machines, and data will continue to drive a new industrial revolution where individuals and enterprises maximize the value of ever-expanding data sets to drive economic growth.

To deliver on these benefits, wireline networks (specifically, fiber optic networks) need to continue to densify, so incentives for rural broadband, along with access to rights-of-way and utility poles, will continue to be essential. The flexibility and adaptability needed for AI-enabled SDN requires robust standards to ensure interoperability. Wireline networks will rely on a trusted supply chain for both hardware and software even as network components evolve. Finally, as future adversaries also adapt to this more connected ecosystem, service providers and enterprise AI-powered security systems must stay ahead of this evolving threat landscape. Doing so will require ongoing access to robust sources of actionable threat data, including U.S. Government intelligence.

Satellite Segment

The space communications segment is experiencing explosive growth in low-earth orbit (LEO) satellites, promising to bring network connectivity to previously unserved communities worldwide. StarLink has already launched over 1,200 satellites and has plans approved by the International Telecommunication Union (ITU) to put 12,000 satellites in orbit. They have also filed plans requesting an additional 30,000 satellites. Iridium recently refreshed its constellation with 75 Iridium NEXT satellites in LEO, completing the set in 2019. Although the LEO growth has received the headlines, geosynchronous earth orbit communications companies such as Intelsat, ViaSat, and Inmarsat continue to provide broad communications coverage and are upgrading their fleets to track emerging terrestrial standards, including adoption of 5G. Inmarsat plans to launch two additional highly elliptical orbit (HEO) satellites in 2022. These will serve the increased air and maritime traffic in the high north.

This growth creates potential benefits to NS/EP missions. Most straightforward is the ability to use satellite bandwidth to recover from the impact of terrestrial networks damaged by disaster and provide access to those communities affected. With global coverage and inexpensive access terminals, commercial satellite communications can mitigate lost terrestrial networks quickly and provide essential communications as terrestrial services are being restored.

Beyond communications, the space segment is seeing expansion of sensing satellites. Commercial imaging in the visible spectrum has seen steady growth for two decades, but other modalities such as infrared, synthetic aperture radar, multispectral sensing, and radio frequency (RF) emissions are all coming online. These other satellite remote sensing services can also be leveraged for NS/EP purposes by enabling detection of large heat sources (e.g., forest fires), advanced imagery despite obscuring weather or darkness, and real-time spectrum usage data.

Although not in orbit, tethered aerostats can complement satellites, providing communications and forming a platform for persistent connectivity. They can carry substantial payloads and can be reconfigured as a situation changes, but are immobile once aloft, so they cover a much more limited area of interest. Aerostats have been used successfully for intelligence, surveillance, and reconnaissance and communications by the DoD and the Department of Homeland Security (DHS) for almost 20 years, and occasionally in natural disaster response as well. In 2019 AT&T launched FirstNet One, a 55-foot aerostat specifically designed for reconstitution and augmentation, and a complement to airborne and satellite methods. The barriers to entry are low relative to space communication, and as a result, there are numerous providers and integrators, both domestically and overseas.

As the commercial space market has matured, the military and Federal Government have utilized commercial satellite services and integrated them into their operations. This trend should accelerate with the growing scope and scale of commercial space. The military and Federal Government also have long

commissioned and operated the world's most extensive satellite capabilities and are often early adopters and sponsors of the best in commercial and academic advances to stay ahead. For example, just recently the U.S. Space Force's Cross Mission Ground and Communications Enterprise Directorate, seeking to improve space communications by borrowing from advances in 5G technology, issued a request for information.[15] Both direct use of commercial services and the adaptation of commercial technologies into bespoke Government solutions can benefit the resiliency of NS communications through improved interoperability.

Wireless 5G/6G

Over the next decade, many innovations will make the leap to fifth generation (5G) and sixth generation (6G) networks possible and enable more powerful networks in the future. 5G deployment experience will bring enhancements to network slicing and private networking that will become standard in 6G, enabling new use cases for consumers, small and medium businesses, large enterprises, and Government agencies. A network slice is a logically isolated network that is configured to provide the required network resources for a defined purpose. That purpose will evolve from support of endpoint-based use cases to support of application-based use cases, enabling network slices to be configured to provide the precise performance, quality of experience, and security needed for the service being supported. Networks will be further logically isolated using private networks to meet the security, integrity, and resiliency requirements of specific customers, such as enterprises, Government agencies, or military units. An example of a use case that will benefit from these advances in network slicing technology is mission-critical services for public safety, ensuring dedicated resources, specialized applications, and tailored security while sharing commercial infrastructure.

The next decade will also bring advances in multi-user, multiple-input, multiple-output (MU-MIMO), carrier aggregation, and dynamic spectrum sharing (DSS) technologies, along with advances in mmWave, 100Ghz, and THz frequency spectrums to enable new use cases. MU-MIMO connects each device to multiple antennas and is coupled with beamforming to increase densification (more devices to the same cell infrastructure) while delivering faster data speeds to each device. 5G CA enables support for the 5G uplink operating on a lower band, with the 5G downlink operating on a mid or high band to provide the ideal blend of coverage, capacity, and data speeds. DSS enables operators to share the spectrum for fourth generation (4G) and 5G (and presumably 6G in the future) to facilitate the transition between the technologies. Using advanced antenna system technologies, mobile operators will be able to provide greater coverage and higher performance, benefitting public safety, enterprise IoT use cases, and consumers.

Recent advancements in Microwave Amplification by

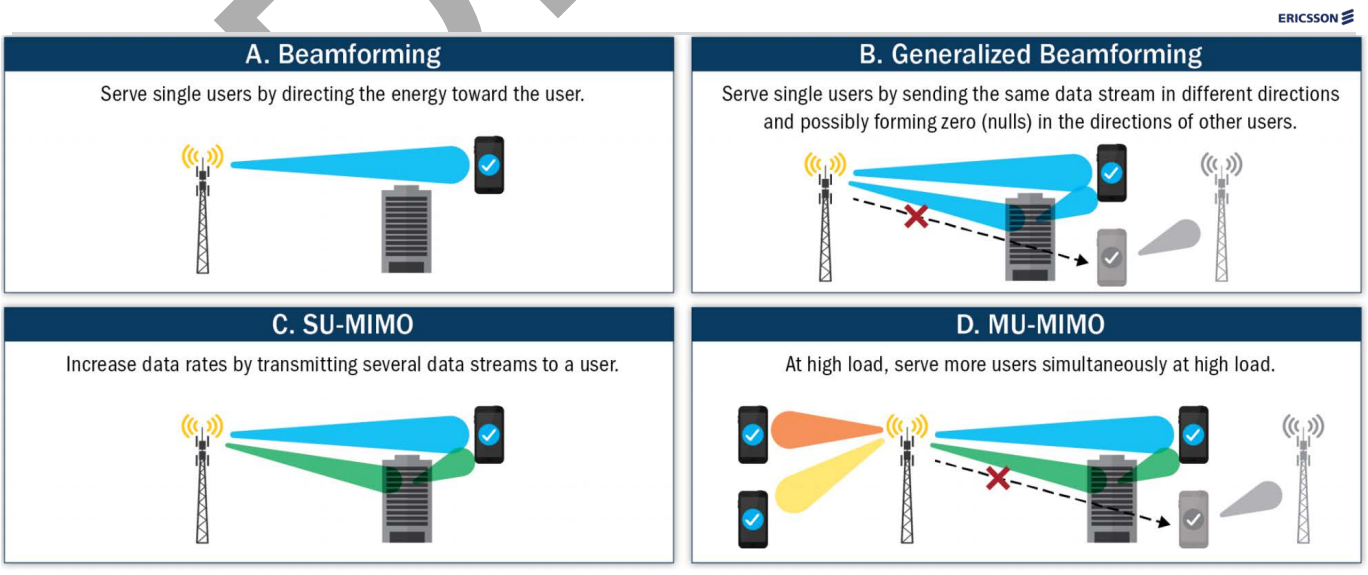

Figure 2. Advanced Antenna Systems – Beamforming and MIMO Examples[16]

[16]Ericsson, Advanced Antenna Systems for 5G Networks, https://www.ericsson.com/en/reports-and-papers/white-papers/advanced-antenna-systems-for-5g-networks

Stimulated Emission of Radiation, essentially a laser in radio/microwave bands, technology have opened a path toward large wireless power transfer between two endpoints, allowing immediate restoration of wireless communication in disaster areas. Restoring wireless communication can be accomplished without the need for restoration of power by recharging the devices in the field remotely or transferring power wirelessly to remote terrestrial or airborne equipment.

Public Safety Communications

The densification of networks, ubiquitous connectivity, and accelerating incorporation of sensors and IoT devices will bring profound changes to public safety communications. First responder voice communications will remain vital and will be met through a combination of the National Public Safety Broadband Network (NPSBN), other commercial 4G and 5G offerings, increasingly meshed "smart" land mobile radio (LMR) systems, and non-terrestrial networks (NTN). The addition of data services to connect sensor networks, deliver real-time video, and provide critical data resources will revolutionize public safety communications. These developments will provide responders with real-time situational awareness and incident leaders with unprecedented ability to rapidly understand evolving emergencies so that the best possible combination of resources and information can be directed where needed most.

For the general public, the same densification and ubiquitous connectivity will help ensure the ability to contact emergency services, stay informed of developing emergencies near them, and remain in touch with family during emergencies. Expected improvements in location services will increase the ability to dispatch responders directly to the scene of the emergency, and adoption of Next Generation 911 capabilities will afford the public more robust and varied means to communicate distress and situational awareness directly to authorities. With increased adoption of the Advanced Television Systems Committee (ATSC) 3.0 standard, broadcast communications will increasingly be available to "data cast" critical public safety information such as emergency alerts with maps and detailed instructions.

To deliver on these opportunities, networks must provide the bandwidth and latency necessary to move such a significant amount of data in the most demanding circumstances, including when the networks or their supporting infrastructures are themselves damaged or degraded. Doing do will require well coordinated wireless and wireline networks with resilience built in through redundant paths, physical hardening, appropriate back-up power capabilities, plentiful and available spectrum across multiple bands, and data/voice priority services such as Precedence and Preemption and QoS. Distribution of network cores closer to the edge, enabled by virtualization, can provide faster response times with lower latency and greater network resilience. Resilient and enhanced location services—likely beyond simple Global Positioning System (GPS)—will be needed to provide location accuracy, particularly in indoor and urban settings.

Usage of the massively increased available data from biometrics, video, IoT sensors, unmanned vehicles, etc. will require a range of capabilities, including public safety-grade edge computing, artificial intelligence/machine learning (AI/ML), and enhanced human-computer interface methods such as haptics, heads-up displays for responders, and augmented reality integration. The public safety communications ecosystems will need to leverage a distributed core that integrates seamlessly into a single, geo-redundant architecture covering multiple emergency systems, such as the NPSBN, Next Generation 911, and computer-aided dispatch and multiple access technologies, such as LMR, NTN, long-term evolution, and 5G.

Key Evolutions in the Power Sector

Just as the communications sector moved from a hierarchical to a distributed architecture, so too is the power sector evolving toward the "Smart Grid,"[17] an interoperable, multi-distributed network. As described by DoE:

> Today, [the network] consists of more than 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines. Although the electric grid is considered an engineering marvel, we are stretching its

[17]Department of Energy, "The Smart Grid," https://www.smartgrid.gov/the_smart_grid/smart_grid.html

patchwork nature to its capacity. To move forward, we need a new kind of electric grid, one that is built from the bottom up to handle the groundswell of digital and computerized equipment and technology dependent on it—and one that can automate and manage the increasing complexity and needs of electricity in the 21st Century.

Similar to the transformation of the ICT ecosystem, advances in a number of technologies, including advanced instrumentation, relays, sensors and switches, battery storage, smart meters, and renewable energy sources are enabling this evolution. When coupled with the power sector's increased emphasis on more commodity-like infrastructure elements such as smaller, interoperable transformers, the power sector will increasingly look more like an SDN-enabled operation within the United States.[18] Among other things, the benefits of this evolution include quicker restoration of electricity after power disturbances;[19] more efficient transmission of electricity; increased integration of large-scale renewable energy systems; better integration of customer-owner power generation systems, including renewable energy systems;[20] and improved security.

The power and ICT sectors share mutual dependencies. While the communications sector has extensive back-up power in place to ensure ongoing operations, not every network element lends itself to this type of protection. As the industry moves to a 5G/Next-Gen environment, it is unclear to what extent this reliance on power becomes exacerbated or mitigated, particularly given the billions of IoT devices that may be elements in critical services. In short, while the Smart Grid enhancements will undoubtedly improve the resilience and reliability of power for ICT purposes, it will not reduce ICT's reliance on this critical function.

In turn, the power sector relies on ICT to manage the generation, transmission, and distribution of their own systems. While the power sector owns and operates private communication networks and is not wholly reliant on commercial capabilities, the proportion of private to commercial infrastructure will shift significantly during this change to the Smart Grid. These operational dependencies remain critical and indicate that forward-looking assessments should be conducted to determine how the power, IT, and communications sectors could interact to become better informed and collaborate to assure the delivery of each sector's critical functions. While work within DHS' National Risk Management Center (NRMC) is already underway to better understand the dependency and interdependency of cross-sector critical functions, collaborating now to assure future outcomes could drive more automated or sensor aware solutions while each sector is still in the early stages of this evolution.

Next-Gen IP

Emerging applications such as real-time video analytics, tactile internet, and virtual reality will continue to drive the innovation necessary to deliver high-performance networking and computing. The next generation of performance-sensitive IP networks will be supported by multiple large-scale backbones, hyperscalers, and content delivery networks (CDN) sharing flatter interconnection – including geographic distribution of data centers – to deliver the latency, loss, and bandwidth requirements needed for future applications. These next generation networks will have more robust connectivity, with fiber to the home expected to hit 70 percent by 2030, and 5G/6G/Wi-Fi/satellite connectivity used where fiber does not reach. This hyperconnected network will both enable and rely upon an expansion of today's cloud environment: leveraging edge computing to drive lower latency and multi-cloud/private cloud to provide security, resilience, and scale for future applications.

The next generation of on-demand networking, managed through SDN, will rely on standards and interoperable service APIs to support future use cases, but current IP networking protocols may not be

[18]National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0" February 18, 2021, https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40

[19]National Institute of Standards and Technology, "Quantifying Operational Resilience Benefits of the Smart Grid," February 2021, https://www.nist.gov/publications/quantifying-operational-resilience-benefits-smart-gridx

[20]Susser, Jonathan, Advanced Energy, "The Evolving Electric Power Grid," February 27, 2020, https://www.advancedenergy.org/2020/02/27/the-evolving-electric-power-grid/

deterministic enough to provide the latency guarantees necessary to support these future use cases. The Internet Engineering Task Force (IETF) has discrete efforts underway to address many of these future performance requirements. Huawei's "New Internet Protocol," or "New IP," initiative reflects many of these future performance concepts but carries risks due to its top-down design, lack of parallel implementation within current internet protocols, potential for undesirable state control of and visibility into network communications, and reinforcement of nascent bifurcation of the internet already underway. Section 4.2.1 provides a more detailed discussion of potential issues related to New IP. The IETF has expressed significant concerns with the New IP proposal.[21]

ICT Architectures Transformation

Role of Hyperscalers

Hyperscalers achieve massive scale in computing, utilizing a dynamic, flexible server architecture and virtual networking functions, typically in support of services that rely upon big data, AI, or cloud computing. Hyperscale infrastructure is designed for horizontal scalability (adding more servers/machines to a pool of resources) instead of vertical scalability (adding more compute/memory to an individual server), leading to high levels of performance, redundancy, fault tolerance, and extensibility. This growth is driven through two technologies: Internet Exchange Points (IXPs) and CDNs. IXPs provide direct peering among networks, thus reducing dependence on traditional Tier 1/Tier 2 Internet Service Providers (ISPs). IXPs are the physical infrastructure through which ISPs and CDNs exchange internet traffic between their networks. The primary purpose of an IXP is to allow networks to interconnect directly via the exchange, rather than through one or more third-party networks. The advantages of this direct connection are cost, latency, and bandwidth. CDNs are owned and operated by numerous entities within the ICT ecosystem (including the ISPs) and are utilized to either optimize the entities' own traffic or, alternatively, to provide pathways for entities that have high bandwidth requirements but insufficient need to operate their own network. "IXPs have facilitated the bypassing of Tier-1 transit providers."[22] This trend suggests that the traditional hierarchical routing through Tier1/Tier2 ISPs is becoming increasingly sidelined to CDNs. Hyperscalers are essentially building their own global network incorporating IXP and CDN capabilities into a fully integrated system.

Cloud Computing

Virtually every aspect of society and the economy will have some dependence upon the real time functions of a small number of public cloud services and cloud service providers (CSP). For these CSPs, software design, architecture, and quality of care are essential to their business function, along with the degree of AI, automation, and processes around change management in their services. Public cloud providers have developed the ability to rapidly change without introducing instability, enabling the digital economy to drive innovation. Automated management (sometimes called orchestration) for dynamic change of allocated resources is a foundational capability for these large cloud providers, which in turn enhances resilience through adaptiveness. However, the ubiquity and complexity of the public cloud has introduced new, and often poorly understood, interdependent risks. This convergence between traditional digital communications and public computing infrastructure has to date not been well understood among regulators, providers, and customers.

Resiliency assessments of traditional telecommunications networks have historically been difficult, even though these networks were significantly simpler than today's digital infrastructure. Further, the architecture of the cloud defies traditional methodologies of risk analysis about the degree and forms of dependency, the identification of single points of failure, and the prediction of emergent behaviors. As difficult as it was to assess the true impact of risk for traditional networks, cloud deployments create new types of risks but also provide the financial means for a deeper investment in resiliency and security.

[21]IETF, Liaison statement: Response to "LS on New IP, Shaping Future Network," March 30, 2020, https://datatracker.ietf.org/liaison/1677/

[22]Antichi, Gianni et al., "The Elusive Internet Flattening: 10 Years of IXP Growth," November 7, 2018, https://www.researchgate.net/publication/328528921_The_Elusive_Internet_Flattening_10_Years_of_IXP_Growth

Edge Computing

As more and more devices, sensors, and equipment become networked, edge computing enhances the ability of enterprises to derive value from data, facilitating the acquisition and storage of data from ever increasing networked sensors and devices, providing sufficient computing power to analyze that data quickly, and returning that information to the enterprise to act in near real-time. To deliver on this vision, edge computing brings processing and data closer to the point of digital interaction to deliver higher performance with lower latency. Edge implementations vary based on the requirements for latency, processing, and data: Applications requiring sub-millisecond response may require on-premises edge solutions, while market/metro-area edge architectures deliver latencies in the five to ten millisecond range. According to Gartner,[23] a massive transition is underway from the cloud to the edge, with overall workloads shifting from 90 percent cloud in 2020 to 75 percent edge by 2025.

Edge computing combines aspects of localized/on-premise computing and cloud for many operational activities while minimizing the downsides of both. Edge computing's low latency enables near real-time performance for applications such as AI-powered semi-autonomous manufacturing, "smart" cities, video streaming analytics, and augmented reality. At the same time, moving computing off the device allows inexpensive IoT devices and sensors to both contribute to and benefit from the richness of big data and high-powered analytics. Edge computing, particularly in the market/metro area, also provides some of the physical security, redundancy, and business continuity capabilities of traditional cloud operations while keeping data and compute resources closer to where they are used, decreasing latency and facilitating data regulatory compliance.

Edge computing delivers the highest benefits in an ecosystem of hyperconnectivity with a robust, interconnected architecture of deployed fiber and dense wireless networks. Software-defined networking abstracts this physical architecture, enabling the provisioning and network management tools necessary to rapidly and flexibly harness the power of the physical networks. Flatter and more deterministic interconnections will further enable the future multi-cloud/edge environment, with enterprise applications positioned at the optimal multi-cloud location for their data, processing, and latency requirements using network and security orchestration tools to provision and secure these data, network, and computing resources.

In terms of trustworthiness, these networks should also be able to leverage new confidential computing technologies, improve service availability, and provide enhanced security identities and protocols with end-to-end assurance. These networks will need the capabilities of local computing integration and infrastructure that enables distributed applications and network functions to be swiftly developed and deployed. Services for data and computing acceleration can then be delivered throughout the network with performance guarantees. NSTAC expects many enterprises will choose to leverage this form of distributed processing in the coming years to enable more robust and resilient operations as well.

Shifting Focus From the "Last Mile" to the Enterprise

The "last mile" has historically referred to the final leg of the network that delivered service to the end user (customer). Over time, this "last mile" has changed from being a copper circuit between the end user's home or office, to now more likely being wireless signal between the user's wireless device and the closest cell site or a high-speed fiber optic connection. From the perspective of the end user, this "last mile" had the highest potential of being a single point of failure, for if that connection was disrupted, the end user's service was disrupted as well. To ensure continued access to network services, end users with highly critical connectivity needs added alternative "last mile" paths to the public network. In addition, programs were developed to identify which "last mile" circuits might be more critical to the community so that those circuit's restoration would be prioritized after failure.[24] Diversity in routing between the end user (enterprise) and the public network will continue to remain a critical

[23]Van der Meulen, Rob, Gartner, "What Edge Computing Means for Infrastructure and Operations Leaders," October 3, 2018, What Edge Computing Means for Infrastructure and Operations Leaders - Smarter With Gartner

and foundational best practice to ensure the resiliency or continuity of the enterprise. As the networks evolve, this foundational practice will not change. What will change is the enterprise's ability to leverage the very same principles used by the ICT providers to create an equally resilient and distributed architecture, managed directly by the enterprise. This evolution in approach, from the enterprise focusing on last-mile single point of failure to the enterprise leveraging the full capabilities of the ICT ecosystem, will make the next decade focused on the enterprise and their evolution. This section will focus on the role of the enterprise in this new ecosystem, the environment they face, and what will be required for the enterprise to become the source for innovation.

The enterprise-centric ecosystem will represent a significant shift in roles for all players. While relationships between the enterprise and ICT vendor were generally bilateral, the innovation opportunities presented by the countless number of enterprises will provide the ability for any enterprise to assemble the portfolio of ICT platforms, applications, and service providers most appropriate for them. In short, a major feature of the enterprise-centric shift to next generation capabilities will be the partnerships and ecosystems designed to meet the customer's unique goals for digital transformation. The access, edge, and cloud providers are assembling a portfolio of pre-screened, trusted partners that they can operate with, and this transition to treating these large assets as a platform for innovation is already underway. "We are making the investments in platforms and IT systems to create the 'network as a platform.'" The transition means having most customer requests as ready-to-go, off-the-shelf solutions and helping customers plug in and innovate. "It's about building a series of foundational capabilities and allowing applications to flourish on the network. We are not going to be the experts in every vertical—what we need is to be experts in having an exposed set of capabilities to allow those verticals to plug into us."[25]

The COVID-19 crisis was characterized by an accelerated shift to remote work and has provided insights into threats the work environment of the future may face. The remote work environment, coupled with a wide diversity of end-point equipment, portends the potential for a massive expansion of the attack surface. Recent supply chain events also demonstrate how a sophisticated, patient, and persistent attack through presumed-good software providers or the exploitation of zero-day vulnerabilities can have a chilling impact. In these cases, addressing the identification and mitigation of the breach required trained professionals. The cybersecurity challenges brought into sharp focus by the COVID-19 crisis and recent supply chain compromise will continue to vex enterprises and organizations as ubiquitous, on-demand connectivity and the exponential growth of connected assets increase over the next decade.

Given the increasing presence of highly sophisticated threat actors, compounded by the lack of trained professionals in key technologies, NSTAC anticipates enterprises will fall into three size related categories: very small, small-to-midsize with significant compliance requirements, and the larger enterprise that is able to fully leverage next-generation ICT capabilities to optimize their business model. In each case, these enterprises will rely upon ICT providers to better assure their security.

- For small companies with limited compliance requirements, use of unified threat management (UTM) capabilities via hardware, virtual appliance, or cloud service will continue to expand. The UTM capability can provide multiple network security functions, including firewalls, intrusion prevention systems, secure web and email gateways, remote access tools, routing, and Wide Area Networking (WAN) connectivity. The value of this type of hardware or service is that it protects businesses from security threats using a simplified approach, requiring less individual expertise across multiple systems.
- For small or midsize companies with higher levels of regulatory or compliance requirements, a more comprehensive approach may be required and would be provided using managed cybersecurity and compliance support. These services generally blend some form of UTM capability referenced above. They

[24]Cybersecurity and Infrastructure Security Agency, "Telecommunications Service Priority," January 23, 2020, https://www.cisa.gov/telecommunications-service-priority-tsp

[25]Brock, Alexander, Yoon, Kim, MIT Technology Review, "5G and the Enterprise Opportunity," October 7, 2020, https://www.technologyreview.com/2020/10/07/1009178/5g-and-the-enterprise-opportunity/

also perform many of the roles generally provided by a chief information security officer to ensure that frameworks are in place to meet regulatory requirements, compliance certifications, and business-level cybersecurity standards.

- The final category will comprise companies that will realign their enterprises to become more distributed by leveraging the same techniques that the ICT entities have used to create their own platforms.

In the first two cases, enterprises will be highly reliant upon the inherent security and capabilities of the ICT service providers and clear understanding of who is responsible for which aspects. Understanding the risk associated with reliance upon UTM or managed cybersecurity and compliance support will remain the responsibility of the enterprise, no matter how small. Efforts to create common taxonomies or frameworks to communicate what practices are taken by these ICT providers need to be refined to ensure the enterprise understands both the risks and benefits associated with this approach.

Even with such reliance, the enterprise will still need to assume responsibility for key security aspects of its own operations.

> Most notably, the enterprise must provide for the security of its own devices and endpoints, as well as the data and applications within. This includes all endpoints, IoT devices, multi-access edge compute devices, applications, and more. The customer—or organization at large in this case—is responsible for the security of the data that they create and store on the network. Additionally, enhanced identity access management and data protection suites are needed in addition to the physical security of any on-premises customer equipment used…[26]

There is no single path to transform the enterprise, for the reasons to undertake this journey and the diversity of the enterprise's people, processes, assets, and data will remain unique to that organization. Nonetheless, the activities to begin this transformation will require looking at the architecture of the enterprise as well as the security aspects in a different way to enable the benefits of this new approach: the ability to create new business models leveraging the low latency and high bandwidth characteristics of the ICT platform.

As the enterprise begins this transformation toward a more distributed and automated environment, initial assessments of current systems to determine which infrastructure is SDN-capable or can be updated to this capability should be considered. Replacing legacy systems not capable of supporting future transformation should be considered as well. Some of the current environments to review include the enterprise's current use of data centers or cloud environments, converting applications to cloud-native microservices, and converting networking equipment to support SDN/NFV management of those services. Other initial architecture steps might include reviewing the enterprises' current networking to incorporate software-defined wide area networking. By implementing this capability, the enterprise will begin to see immediate benefits in their ability to actively manage network paths, bandwidth, and latency for their operations. At a higher level, the review of the enterprise architecture should consider incorporating cloud and edge computing into the enterprise architecture. Over time, the enterprise will be able to use the full capabilities of SDN/NFV orchestration to automate and dynamically respond to changing environments.

Organizations wishing to leverage next-gen capabilities to optimize and customize their operations will need to adopt a defense-in-depth and risk-based vulnerability management (RBVM) approach to ensure their operations remain secure. Among other things, RBVM practices include knowing the full range of connected assets on a network, continuously monitoring these assets, deploying user and privileged access monitoring for connected devices and systems, and prioritizing vulnerability remediation efforts based on risk-based contextual factors (severity, exploitability, asset criticality, and data classification).

Leveraging next-generation network capabilities, edge implementations, and cloud environments

[26]AT&T, "Cybersecurity Insights Report, Tenth Edition: 5G and the Journey to the Edge," 2021, https://cdncybersecurity.att.com/docs/whitepapers/cybersecurity-insights-report-tenth-edition.pdf

along with ubiquitous connectivity will, however, enable enterprise-specific platforms to deploy faster, more dynamically, and more efficiently. As an enterprise leverages other platforms and relies on that infrastructure to execute their mission, it will be essential to build holistic security to close the exposure gap. Taking advantage of the resiliency and operational benefits while combatting new and emerging threats will require developers, users, and service providers to partner and operate within the ecosystem of trusted vendors/providers chosen and customized for that enterprise.

ICT Security Transformation

New technologies and innovations will continue to bring advancements to the realm of security, in both defensive capabilities and adversarial tools. Over the course of the next decade, certain security mitigation techniques and technologies must continue to be developed and deployed throughout the ICT ecosystem.

AT&T Response to Nashville Bombings

On Friday, December 25, 2020, at approximately 6:30 a.m., a bomb detonated from inside a vehicle parked in downtown Nashville, TN, near an AT&T network facility housing critical infrastructure. The explosion damaged more than 40 local buildings and left a crater on the east-facing side of AT&T's building on 2nd Avenue North. Unlike many other buildings nearby, AT&T's heavily hardened facility remained structurally stable. The blast knocked out commercial power and destroyed the power infrastructure that linked to the fixed backup generators. Despite the building's proximity to the blast and the power infrastructure damage, the facility seamlessly transitioned to temporary backup battery power as designed, ensuring continuity in service immediately following the blast. The AT&T networks remained operational throughout the morning. The eventual depletion of temporary battery power before commercial or outside generator power could be restored led to the communications service disruptions across Nashville, Tennessee, and other nearby states in the region, including Kentucky and Alabama.

AT&T's response began within minutes after the explosion; however, access for on-site restoration and recovery work was delayed for up to 12 hours for safety assurance, crime-scene preservation, and evidence gathering. Experienced employees and Network Disaster Recovery (NDR) and FirstNet teams executing disaster response plans in close cooperation with federal, state, and local public safety agencies and officials were critical elements for a rapid recovery. Prior to losing power, AT&T quickly mobilized to triage and scenario plan. Technical teams worked remotely to reroute services and shut down non-essential equipment to conserve temporary battery power. Operations teams focused on facility recovery, including prioritizing and mobilizing resources such as portable cell sites (Sat COLTs) – the first Sat COLT deployed was on air serving first responders in the immediate blast area within 4 hours of losing power. During this event, a total of 24 portable cell sites were deployed or staged, and, at the peak, 21 were on air simultaneously. National network traffic flowing through the Nashville hub automatically rerouted; however, traffic terminating or originating locally through this hub was impacted when power was lost. Most 911 rerouting for PSAPs was completed within 12 hours of losing power. Engineering teams working around the clock completed a major wireless traffic manual rerouting effort within 24 hours, restoring approximately 25 percent of mobility sites. Within 36 hours and after drilling holes through concrete walls and laying temporary new cables, an outside generator began providing power to the building. Most communications services were restored within 48 hours of losing power, and remaining services were fully restored in the following days.

STATEMENT:

To help reduce impact from a potential service disruption, enterprises should take into consideration fallback routing for their critical functions as they develop and/or review their business continuity plans.

Subsequently, they should also be adopted by U.S. Government networks and mastered at a high level if the Nation is to not only keep pace but try to stay ahead of emerging threats.

Zero-Trust Adoption

The security model known as "zero-trust" uses an identity-centric approach for mutual authentication that assumes all requests are inherently "untrusted," even if they are entirely within the traditional perimeter of the network. Policy-based authorization decisions are combined with traditional security principles and contextual factors to vet traffic at every step of the network path, limiting potential consequences of both cyber breaches and insider threats through precise risk-based access controls for each decision to access or change data, assets, applications, and services. National Institute of Standards and Technology (NIST) Special Publication 800-207, the Cybersecurity and Infrastructure Security Agency's (CISA) Trusted Internet Connections Initiative, and the United Kingdom's National Cyber Security Centre, align with key principles of a Zero-Trust Architecture (ZTA), and DoD's Cybersecurity Maturity Model Certification is driving accelerated zero-trust adoption.

While further effort is needed to align the integration or interconnection of the numerous elements, systems, and networks that are moving in this direction, harmonization of ZTA best practices and standardized configuration and integration guidelines should allow for more predictable and interoperable systems that use ZTA in the future.

Denial of Service (DDoS) Mitigation

Distributed Denial of Service attacks show no signs of slowing over the next decade, and the addition of billions of IoT devices will provide additional attack vectors and increase the volume of DDoS attacks. The Council to Secure the Digital Economy has framed a collaborative approach to Botnet mitigation across enterprises, device hardware and software manufacturers, and infrastructure operators.[27] Twelve major network and CDN providers working in concert will leverage Border Gateway Protocol and Domain Name Service redirection to "clean" DDoS traffic. Networked devices should adopt secure by-design software and hardware development processes and life cycle management practices. Enterprises will have a critical role to play in managing the security of their increasing number of networked devices.

Enterprise Protections via SDN

SDN implementation will enable significant opportunities to improve security. SDN's centralized control standardizes security perimeters through universal policy application across domains. This software centric approach allows for fine-grained policy and traffic control specific to an application and session instead of a physical network topology. Micro-segmentation allows for the separation and granular control of virtualized data center components and workloads, further protecting against lateral movement and allowing easier application of security policies to specific segments and workflows. SDN also allows for a greater degree of automation in security management and response: The increased network visibility will provide large data sets that facilitate AI-powered threat detection that will, in turn, drive real-time automated response and traffic containment. Finally, SDN will become the foundation to seamlessly integrate and operate future zero-trust environments through its support for granular authentication and ability to tailor policy constraints.

Integrity Protection and Security Assurance

The end-to-end integrity of software and hardware, from origination in the supply chain, through design and integration and, ultimately, in implementation within the network, will be crucial to the security and resilience of future critical infrastructure. Leading-edge practices in secure software development using DevSecOps (the integration of security into development operations) should become commonplace in future ICT solutions; these include signing of software, secure distribution methods, a traceable DevOps path, and cryptographic attestation of integrity delivered via public key infrastructure or distributed ledger (e.g., blockchain) technologies. Similarly, verifying the authenticity and

[27]Council to Secure the Digital Economy, International Botnet and IoT Security Guide 2021, https://securingdigitaleconomy.org/projects/international-anti-botnet-guide/

trustworthiness of hardware will rely on a chain of trust that can be cryptographically anchored from the chipset up through the components and into the firmware and operating system. This trust anchor can be tied to applications running on the platform as well, ensuring that only known, signed services can be instantiated. The attestable state of a system, at both the software and hardware levels, can provide an attributable mark of trustworthiness that can be used in orchestration decisions within the network, as well as deterministically in policy-based ZTAs. To achieve this end state, further work refining the more secure development environments and life cycles for this next generation of capabilities is needed. Such processes would incorporate elements of the following: (1) trusted flow of resources (silicon/chipsets/materials); (2) standardization; (3) design; (4) validation/testbeds; and (5) testing. Testing would entail cataloging internal hardware and software bill of materials and external attestation of trusted components.

Major Technologies and Resources Leveraged

Software-Defined Networking

As reflected in the 2020 *NSTAC Report to the President on Software-Defined Networking* and the 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision*,[28] SDN and related NFV technologies are revolutionizing network operations across the globe. SDN and NFV have enabled a sustained transition from legacy hardware-based networking technologies to software-based networks that run on more standardized, commodity-based hardware. Carriers, service providers, and public and private sector enterprises are increasingly using SDN. SDN adoption by the enterprise has accelerated via wide area networking solutions to deliver high-performance wide-area networks via lower-cost, commercially available internet access. The buildout of 5G mobile infrastructure is software-centric and virtualized. As such, SDN plays a critical role in networking the various service-based applications in 5G implementations.

Network virtualization provides significant performance, flexibility, adoptability, resiliency, security, and cost advantages. SDN allows a move from dedicated hardware-based architecture to less expensive, more flexible systems in which the primary value is provided by software, reducing product development cost and time, lowering market entry barriers, spurring investment, and promoting innovation. SDN enables security innovation by facilitating the real-time incorporation of security features using artificial intelligence to rapidly detect and mitigate malicious activities. Since cloud and edge architectures are heavily reliant on SDN, incorporation by providers simplifies operationalization of operational capabilities for disparate customers. Service providers across the wireline, wireless, and cable sectors identified SDN as a critical enabler of their success in rapidly adapting networks to meet the profound changes in the ICT environment caused by COVID-19 and the related shifts to telework, remote learning, and distance medicine.

While industry adoption of SDN is well underway, there are several enabling capabilities necessary to maximize improvements to security and reliability for NS/EP communications. Standardized interoperability features across all elements of SDN will enable multi-vendor architectures and inter-network compatibility; accordingly, robust U.S.-based investment and innovation in SDN standards development and related technology are critical. Operators must evolve corporate cybersecurity and software maintenance methodologies to take full advantage of SDN's ability to utilize AI and automate security tasks. SDN software, as well as the lower cost commoditized hardware it enables, must come from trusted suppliers. As with any major shift in technology, SDN requires a future workforce with SDN-specific skillsets.

Quantum Computing, Communications, and Encryption

Innovation will continue to drive both the global economy and the Nation's security, and developments in quantum computing, key generation, and communications are a critical component of that required innovative growth this decade. Quantum is a key component of China's computing and communications plans. It must be studied, funded, and coordinated among public, academic, and commercial efforts to meet the goals of the Nation.

[28]National Security and Telecommunications Advisory Committee, "NSTAC Report to the President on Emerging Technologies Strategic Vision," July 14, 2017, https://www.cisa.gov/publication/2017-nstac-publications

After decades of mostly theoretical advancements, quantum computing is poised to affect ICT for generations. While quantum technology and its associated uses are still in the early stages, they are already delivering useful and resilient optimization solutions, such as autonomous robot pathing, network resource planning, inventory management, and distribution logistics, that will soon find their way into the collective infrastructure. The most probable entry path is a "hybrid compute" model that combines classical and quantum computing. More than 250 quantum applications now exist, with rapid growth occurring due in part to cloud-based access to the specialty hardware and conditions needed to operate quantum computers. [29]The complex optimization problems to better optimize design and deployment of Next-Gen networks are well suited to quantum computing, but lack of training, education, and experience in how to frame difficult problems in a quantum format pervades. While the quantum computing firms have developed forums to educate and demonstrate how this form of processing can solve difficult and complex problems, a deeper focus on using quantum today to solve problems of the future appears to be taking a subordinate role to research and development (R&D) efforts associated with quantum cryptography and communications efforts.

Widely used public-key cryptography schemes such as Rivest-Shamir-Adleman (RSA) rely on the fact that prime factorization of large integers using classical computers is an intractable problem. Adversary decryption of public key cryptography schemes such as RSA depends on the computational complexity required for brute-force techniques using classical computers. At some point in the future, using quantum computers and Shor's algorithm, which is designed to find the prime factors of an integer, adversaries will be able to break RSA schemes quickly in polynomial time, rather than exponential time. Advancements by organizations in public, private, and academic areas, and by countries that are both allies and adversaries of the United States, allow adversaries to decrypt the Nation's current public key cryptographically secured information in real time or in near-real time.[30,31,32]

Timelines for achieving this capability (either organically or through theft) vary between 2025 and 2035; thus, it is imperative that mitigation be developed, standardized, and deployed in advance. These mitigation efforts fall into two categories: the first using quantum computing itself to create provably secure encryption, and the second being post-quantum cryptography, which uses other techniques—not dependent on quantum computers—to make cryptography that is highly resistant to a quantum-based decryption effort. Public-private partnerships and functional sandboxes are called for to further optimize collective talent and resources. Preparations should begin now to adapt ICT infrastructure and begin to mitigate risk from quantum computing.

Quantum communication is another innovation that will drive both global economic and national security; utilizing techniques such as quantum entanglement prevents eavesdropping by third parties/adversaries. Two or more particles physically separated from each other, such as photons, are considered entangled if measurement of one affects the other at a distance. If an entangled pair of photons is shared between two endpoints, any attempts to intercept the transmitted entangled photons alters the overall system, revealing the presence of the third party, thus ensuring detection of eavesdropping attempts. Quantum Key Distribution (QKD) is a means of secure communication between two endpoints using a shared random key that can be used to encrypt and decrypt messages. Quantum Key Exchange is a protocol developed to accomplish QKD. Quantum key distribution of sufficiently entangled photons ensures provable security based on information theory and key forwarding secrecy between two endpoints. Greater research and testing at a large scale will be needed to push adoption and ensure that these benefits can be realized in the future.

[29]Ley, Daniel, Schwartz, Allison, and Condello, Alexander, D-Wave, "Practical Quantum Computing: Quantum and Hybrid Solutions for Communication Resiliency" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 31, 2020)

[30]The University of Science and Technology of China, "world's first integrated quantum communication network," January 6, 2021, https://phys.org/news/2021-01-world-quantum-network.html

[31]Johnston, Hamish, "Quantum cryptography network spans 4600 km in China," January 7, 2021, https://physicsworld.com/a/quantum-cryptography-network-spans-4600-km-in-china/

[32]Yirka, Bob "Using Drones to Create Local Quantum Networks," January 18, 2021, https://phys.org/news/2021-01-drones-local-quantum-networks.html

Artificial Intelligence (AI)

AI has come into its own as a driving force in the global economy, with applications of machine learning (ML) creating new markets and disrupting old ones. AI and ML allow computers to process more data faster and with reduced risks (e.g., minimizing human error); enable more advanced modeling and simulations; optimize resource utilization; improve medical, financial, and other outcomes; augment human perception; improve machine and human decision-making; and automate tasks and processes.[33] Several areas of rapid advancement in AI are directly applicable to improved communications resiliency in the service of national security and should be implemented where possible.

- The first area is machine perception. Some of the most successful applications of AI have been in extracting entities and objects from sensed data, commonly in the form of visible imagery, but also in other forms of high-volume sensed data such as thermal, radar and other RF emissions, and acoustic information. These advances can be leveraged directly to yield a faster and more complete understanding of a disaster or other national security event at any stage to diagnose more clearly what has been damaged and to track the progress of reconstruction. AI applied in sensemaking (the human concept of gathering information to refine understanding of a situation) across a range of data can be used to create situational awareness, establish norms, spot deviations from norms, and so on. In ICT, as well as many other domains, this would take the form of a common operating procedure.
- Another area of potential benefit is resource allocation management. AI-based optimization can be very effective when applied to such NS communications resiliency problems as network planning, incident response, and bandwidth or spectrum allocation and reallocation. Combined with autonomy, AI agents can act to anticipate resource shortcomings and reallocate on the fly. Partnered with humans, AI can efficiently compose a range of potential solutions to an incident, predict consequences, and present the most favorable courses of action to an operator.
- AI in the form of adversarial reasoning and reinforcement learning techniques can also benefit security missions. Adversarial reasoning could be used to simulate malicious acts or any series of failures of a complex ICT system. With autonomous software agents playing the roles of attacker (incentivized to deny service) and defender/maintainer (incentivized to maximize service levels) in a safe simulated environment, numerous possibilities are explored quickly and then mined for lessons the real system owners can use. The same approach can be used to improve the resilience of software services; the Defense Advanced Research Projects Agency's Cyber Grand Challenge is an excellent example.
- Natural language processing (NLP) is yet another relevant application of AI. In disaster recovery situations, for example, human responders may need to work with unfamiliar systems where the person has a clear objective but is unsure of the command syntax or menu structure. NLP can be used by untrained workers to query complex data sets, perform analysis, and display results, and researchers are working on interpreting spoken intent to infer and direct complex actions across a system.

The examples above focus on communications resiliency and represent a limited set of possibilities. Realizing the full potential of AI will have a transformational effect on many industries and the bigger global economy. A recent report by the National Security Commission Competitiveness in Artificial Intelligence considers these effects and makes strong, far-reaching recommendations for "comprehensive, whole-of-[N]ation action."[34]

Chipset and Foundry (Resource Issue)

If data is the "New Oil" of the information age, then microelectronics is the "New Steel." A vertically integrated microelectronics industry in the United States is critical for development of chipsets supporting all aspects of emerging communications applications, including 5G and 6G waveforms; edge compute; neuromorphic chipsets for developing machine learning, deep learning, and artificial intelligence engines in hardware; enhanced

[33]Doubleday, Justin, Inside Cybersecurity, "Artificial Intelligence Commission recommends major funding shifts to fuel Pentagon AI advances," February 19, 2020, https://insidecybersecurity.com/daily-news/artificial-intelligence-commission-recommends-major-funding-shifts-fuel-pentagon-ai

cybersecurity using in-built encryption engines in hardware; and supply chain integrity using on-chip watermarks in hardware. A secure supply chain to deliver these critical components depends upon unrestricted access to essential raw materials, a skilled workforce to develop new technologies, and the capital and markets necessary to leverage those technologies into products, all supported through open and fair competition based on rules-based systems.

The United States has dominated the microelectronics industry since the advent of the transistor over 50 years ago. During the Cold War with the Soviet Union, microelectronics provided a critical strategic advantage over the enemy, but rapid commercial adoption of the technology at the close of the Cold War led to waning U.S. Government influence. The U.S. Government, previously the most important purchaser of microelectronics, now accounts for less than one percent of the worldwide market. Commercial growth and the subsequent commoditization of microelectronics led to overseas migration of the industry, starting with low-end and low-wage assembly to drive lower costs, then to packaging, and finally to critical fabrication in foundries. Because a modern advanced node foundry requires an investment of billions of dollars, only a few competitors in private industry have the necessary resources and market scale to build and operate such foundries. Other nations' industrial policies supported these massive investments, while the comparative lack of subsidies and tax incentives in the United States greatly accelerated the consolidation and offshoring of these facilities.

China has realized the strategic importance of access to semiconductor technology and invested throughout the end-to-end supply chain to dominate the sector. China holds an outsized dominance in raw materials such as rare earth materials, and has invested heavily in mining and mineral engineering, metallurgical engineering, and material sciences and engineering.[35] China has also invested heavily in university research, developing a highly skilled domestic workforce with a low-wage advantage in labor intensive assembly and packaging of microelectronics. China also has a large pool of domestic consumers for the electronics they produce and export to the rest of the world. Through these investments, the Chinese industrial base, market size, and manufacturing capability in III-V semiconductors has continued to increase, leaving China poised to take a market-dominant position in this critical industry.

While the potential impact to ICT is significant, many critical industries for the United States' strategic security and economic prosperity, such as defense, automotive, power, medical, chemicals, renewable energy, specialty steel and alloys, and aviation, will also be impacted. Recently, a supply shortage of electronics chips had an adverse impact on the automotive industry in the form of reduced production. A chip shortage in 2021 is also likely to affect the ICT industry.[36,37,38]

To counter this strategic threat to a critical industry, the United States must address all aspects of the microelectronics supply chain. Investment in critical mining and mineral engineering of the raw materials needed for electronics manufacturing in the United States is needed. Maintaining the Nation's technological edge necessitates a national policy to incentivize the training and retention of a skilled workforce. Lack of training and a scarcity of the domestic skilled workers necessary for microelectronics research and development has led to U.S. dependence on foreign graduate students in American universities. It is therefore critical to partner with universities and private and public research laboratories to advance new semiconductor materials and microelectronics technologies and develop a skilled domestic workforce for the design, manufacture, and packaging of microelectronics.

The United States also should strive to onshore the most critical microelectronics manufacturing while encouraging development of other foundries among allies and like-minded nations. The U.S. Government should provide federal incentives to private industry for onshoring advanced node sub-12nm foundries

[34]National Security Commission Competitiveness in Artificial Intelligence, "Final Report," 2021, https://www.nscai.gov/2021-final-report/

[35]Hanke, Steve, Yahoo! News, "China Rattles Its Rare-Earth-Minerals Saber, Again," February 25, 2021, https://news.yahoo.com/china-rattles-rare-earth-minerals-113020191.html

for fabrication of semiconductor chips. The United States should work with its European and Asian allies in developing countries in Asia, Africa, and Central and South America to ensure a cost advantage for commercial electronics for non-critical applications. Using high-volume, most-affordable technology for non-critical applications, assembling, and packaging of electronics overseas in developing countries that are close allies of the United States will ensure a large manufacturing base, a reliable supply chain, and a large export market. Congress is currently prepared to address this key national security issue with the "Creating Helpful Incentives to Produce Semiconductors [CHIPS] for America Act," which seeks to strengthen U.S. semiconductor manufacturing and innovation[39] as a first step in ensuring U.S. leadership in this critical key industry for national security. A comparable, smaller effort to ensure unfettered global and domestic access to raw materials such as rare earth elements and III-V semiconductors will also be necessary.

Finally, increasing the resilience of ICT systems and improving the national security posture will also require development of industrial standards for assurance; frameworks for secure silicon standards for design, manufacturing and packaging; maintenance of a state-of-the-art trusted flow; and expansion of the number of ensured trusted suppliers. Measures to track through the supply chain/design life cycle, including methods for device authentication, watermarking/device characterization, and detecting malicious logic, are required. Supply chains can be further protected by monitoring the infiltration of the venture capital industry and other forms of industrial espionage. Supporting an onshore foundry and critical integration capability for advanced packaging will ensure that a supply chain for a mix of commercial and Government use is supported for critical infrastructure.

Potential Resiliency Stressors to the Future Network

This section provides an evaluation of possible future events that would stress and test the resiliency of communications networks as they evolve. NSTAC was asked to review four scenarios: (1) wide-scale Electromagnetic Pulse (EMP) disruptions and outages, (2) PNT disruptions, especially related to GPS signals, (3) long-term outage (LTO) of electrical power, and (4) supply chain-based cyberattack. These stressors to communications networks can emerge from a range of causes, such as terrorist attacks, natural disasters, solar superstorms in outer space, and malware in cyberspace. A common theme among them is the shared dependencies between critical infrastructure sectors and industries, which must be properly understood to develop effective mitigation strategies that enhance resiliency of future networks.

Wide-Scale Electromagnetic Pulse

Wide-scale EMPs have the potential to disrupt communications and cause power outages across large areas of the United States, as well as damage many kinds of ICT systems and devices. CISA states the impacts of an EMP disturbance "are likely to cascade, initially compromising one or more critical infrastructure sectors, spilling over into additional sectors, and expanding beyond the initial geographic regions adversely impacting millions of households and businesses."[40]

There are two kinds of EMP threats: human-made and naturally occurring.

- **Human-made**: An example of a human-made attack would be a nation-state or terrorist group launching a nuclear device at high altitude. For example, the blast from a 100-kiloton single stage fission device detonated at an altitude of 93 miles would produce

[36]Priddle, Alisa, Motortrend, "Ford Cuts F-150 Production Due to Semiconductor Chip Shortage," February 5, 2021, https://www.motortrend.com/news/semiconductor-chip-shortage-automotive-ford-f-150/

[37]Shead, Sam, CNBC, "Carmakers Have been Hit Hard by a Global Chip Shortage — Here's Why," February 8, 2021, https://www.cnbc.com/2021/02/08/carmakers-have-been-hit-hard-by-a-global-chip-shortage-heres-why-.html

[38]Pressman, Aaron, Fortune, "The Great Chip Shortage of 2021: Why Carmakers and Computer Makers are Scrambling," February 15, 2021, https://fortune.com/2021/02/15/chip-shortage-2021-cars-computers-auto-industry-technology-covid-19/

[39]United States Congress, "CHIPS for America Act", June 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3933/text

charged particles that reach Earth, linger in the sky due to Earth's magnetic field, and compromise ICT systems within 850 miles of the detonation. A high-altitude EMP attack of this kind is known as a "HEMP attack."[41]

- **Naturally occurring**: Besides human-caused EMPs, space weather can also damage communications networks and other critical infrastructure. According to CISA, a geomagnetic disturbance (GMD) caused by severe space weather could damage the electrical grid, communications equipment, water and wastewater systems, and transportation modes. A solar superstorm could cause extra high voltage transformers to fail or prematurely age by saturating their cores. Such an event could also shorten the lifespan of satellites by up to a decade, which in turn can have implications for the timeliness and accuracy of GPS information and impacts on other space-based services.

The most common consequences of either type of EMP event would be widespread disruption of unhardened computers, commercial power outages ranging from days to weeks (for space weather) to months (for HEMP). The Nation's reliance on the critical functions that are operated by infrastructures unprotected from this EMP threat would potentially result in large-scale societal impact.

The 2019 Executive Order (EO) 13865, *Coordinating National Resilience to Electromagnetic Pulse*, recognized EMPs as a major threat to national resilience and laid out a four-year program to "prepare for the effects of EMPs through targeted approaches that coordinate whole-of-Government activities and encourage private-sector engagement. The Federal Government must provide warning of an impending EMP; protect against, respond to, and recover from the effects of an EMP through public and private engagement, planning, and investment." The EO goes on to state "the Federal Government shall promote collaboration and facilitate information sharing,… of threat and vulnerability assessments…, the owners and operators of critical infrastructure, and other relevant stakeholders, as appropriate. The Federal Government shall also provide incentives, as appropriate, to private-sector partners to encourage innovation that strengthens critical infrastructure against the effects of EMPs through the development and implementation of best practices, regulations, and appropriate guidance." The U.S. Government is undertaking the initial preparatory work and will ultimately "develop a plan to mitigate the effects of EMPs on the vulnerable priority critical infrastructure systems, networks, and assets."[42]

As such, NSTAC makes no further recommendations pending this prospective engagement on this topic. Early engagement with the IT, communications, and power-related sectors would optimally position those sectors to build these protections now while deployment of next generation networks is underway.

Position, Navigation, and Timing Disruption

"Everyone in the developed world needs precise time for everything from IT networks to communications. Time is also the basis for positioning and navigation and so is our most silent and important utility."[43]

PNT is broadly essential to U.S. critical infrastructure and nearly all sectors depend on it for a variety of purposes. However, PNT is only as reliable as the source, which typically derives from GPS. GPS signals (and the dependent systems) are vulnerable to malicious actors who could disrupt (jam), manipulate, or spoof GPS signals. Natural space weather events, such as a solar superstorm, could also damage enough satellites to reduce GPS accuracy. While GPS signals were never intended to be the Nation's time standard, their low barrier to entry, precision, and wide availability have made them the de facto national reference. At the same time, such wide adoption means their vulnerabilities pose a near-existential threat.

As foreign adversaries mature their digital capabilities, PNT-dependent systems may become an increasingly attractive target due to their ubiquity, particularly within critical infrastructure systems. In response to

[40]Cybersecurity and Infrastructure Security Agency, "Electromagnetic Pulse and Geomagnetic Disturbance," https://www.cisa.gov/emp-gmd

[41]Cybersecurity and Infrastructure Security Agency, "Electromagnetic Pulse and Geomagnetic Disturbance," https://www.cisa.gov/emp-gmd

[42]The Executive Office of the President, "Executive Order 13865: Coordinating National Resilience to Electromagnetic Pulses," March 26, 2019, https://www.federalregister.gov/documents/2019/03/29/2019-06325/coordinating-national-resilience-to-electromagnetic-pulses

these concerns, the White House released Executive Order 13905, *Strengthening National Resilience through Responsible Use of Positioning, Navigation and Timing*, in March 2020. EO 13905 seeks to "foster the responsible use of PNT services by critical infrastructure owners and operators," with "responsible use" defined as "deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government."[44] Comparable to the EMP executive order, a number of U. S. Government initiatives are already underway to better understand which systems or components across all critical sectors are most reliant on PNT. Early discussions with industry, through Sector Coordinating Councils, have begun. Further, the *National Timing Resilience and Security Act of 2017* mandated that the Department of Transportation establish at least one terrestrial timing system to back up GPS services by December 2020.[45]

Consistent with the *National Timing Resilience and Security Act*, the Department of Transportation reviewed non-space-based technologies to provide alternative PNT. A number of these technologies, including eLoran and fiber-based time distribution, were found to be viable, mature technologies. Given the current low cost of incorporating GPS-derived time, there is little market demand for building these alternative capabilities to the size and scale necessary to provide a viable systemic alternative. To address this deficiency, the executive order outlines a programmatic strategy to inform critical infrastructure entities of their vulnerabilities to spur market demand for these alternative services while also leveraging Government procurement to drive development of market alternatives.[46]

Notwithstanding the EO's efforts to drive the development of market incentives, the current source of timing has no cost to the end user, as compared to any "above zero" cost for these alternatives. To improve the efficacy of these market initiatives, the Administration should consider developing a strategy for National Timing Architecture similar to that reflected in the Resilient Navigation and Timing Foundation's paper entitled "A Resilient National Timing Architecture."[47] Further, to enhance the ability of commercial entities to afford leveraging this architecture, the Administration should appropriate sufficient funds to lay the foundation for creating this timing architecture, with the Federal Government being the first customer for what will ultimately become a resilient, interconnected network for PNT delivery.

Long-Term Outage (30+ days)

An LTO is "an interruption of electrical power within a large enough geographical area, and for a period of time beyond the capability of backup power systems currently in use to provide for the continuing operation of communications systems and networks."[48] Given the number of generator and battery backup facilities and the fuel contracts in place, this period is generally in the 30+ day range. Despite its low likelihood, an LTO could conceivably arise from several different causes, ranging from human sabotage by kinetic or cyber means to natural disasters such as an EMP event.

Whatever the cause, a large-scale outage of this duration would have a significant impact on the ability to provide services. The unavailability of electrical power for more than 30 days would have consequences for fuel distribution that make mitigation even more difficult. For example:

- Gasoline and diesel fuel from pipelines may be unavailable if electric power has been lost at the pipeline pumping stations.
- Storage depots in the region affected by the LTO may be unable to supply fuel to distribution

[43]Resilient Navigation and Timing Foundation, "A Resilient National Timing Architecture," October 16, 2020, https://rntfnd.org/wp-content/uploads/Resilient-National-Timing-Architecture-16-Oct-2020.pdf

[44]Executive Office of the President, "EO 13905: Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," February 18, 2020, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

[45]United States Congress, "National Timing and Resiliency Act of 2017," December 2017, https://www.congress.gov/bill/115th- congress/senate-bill/2220

[46]GPS.gov, "LORAN-C Infrastructure and E-Loran", 2019, https://www.gps.gov/policy/legislation/loran-c/

[47]Resilient Navigation and Timing Foundation, "A Resilient National Timing Architecture," October 16, 2020, https://rntfnd.org/wp-content/uploads/Resilient-National-Timing-Architecture-16-Oct-2020.pdf

facilities, such as gasoline and diesel fuel stations.

- Trucks that normally distribute gasoline and diesel fuel to fuel stations may not have fuel for their engines or products to deliver to the fuel stations.
- Without electric power at pipeline pumping stations, natural gas may also be unavailable. As a result, fuel deliveries to the operating backup generators might be suspended until commercial electric power is restored.

At a higher, system level, a large-scale, extended power outage will create significant disturbances in all fuel-related supply chains nationwide, likely triggering "act of god" clauses in the local, regional, and national fuel contracts held by major providers.

Under this LTO scenario, the response activity will focus on procuring fuel, presumably through state and federal stockpiles, to maintain essential services. Both NSTAC and the Communications Sector Coordinating Council have assessed this scenario several times in the past 20 years, so the LTO issues are well understood; however, several critical unknowns would help better inform response planning for this scenario:

1. How much fuel does the Nation have in state/federal fuel stockpiles at any given time?
2. If there are X million gallons of fuel, how long would that fuel sustain the essential services for a state, a region, or the Nation?
3. Under what circumstances could ICT providers (or critical infrastructure operators) get access to that fuel?

Answering the first question appears simple. Determining "how long will the fuel last" will likely require an analysis of what is critical for each state or region and having a better understanding of what the fuel consumption rates are on a daily or weekly basis. This assessment could be conducted under the auspices of DHS's National Risk Management Center, particularly given DHS's outreach role to state, local, tribal, and territorial governments in addition to the private sector. Once the assessment can be completed for the first two questions, then the discussion about whether industry would be given access to those assets and under what circumstances can be explored. Since access to fuel will significantly mitigate the societal impact from an LTO, this analysis seems worthy of the time and resources required to address the questions.

Supply-Chain Based Cyber Attack

The security of ICT supply chains has been a growing area of concern, with foreign adversaries realizing they can gain access to sensitive and proprietary information by discreetly embedding themselves in the supply chains of companies and governments. These types of threats became part of the national dialogue with prior concerns about software suppliers from adversarial nations and more recently reached critical mass following a recent unprecedented supply chain attack involving malicious updates unknowingly distributed by a domestic software company and further zero day attacks on widely used commercial software. Incidents of this type are revealing systemic weaknesses in how the country identifies and mitigates supply chain risks and approaches the asymmetries between cyber defense and cyber offense. They are serving as a catalyst toward fundamentally new approaches to modernizing the Nation's national cyber defenses and strengthening supply chain integrity.

Several near-term actions can be taken now to begin transforming the resiliency of the ICT ecosystem, such that by 2030, supply chain attacks would either be thwarted entirely or their impact on national critical functions mitigated significantly.

The fundamental challenges that must be addressed to mitigate the impact of a future supply chain exploitation are (1) improving visibility into the inputs (hardware, software) provided by partners, vendors, service providers, and integrators, (2) having visibility

[48]National Security Council, "Communications Dependency on Electric Power Working Group Report: Long-Term Outage Study," 2009, https://www.hsdl.org/?view&did=13836

and control over the connection points between systems, networks, applications, edge processing, and cloud, and (3) maintaining operational control over those aspects that manage or orchestrate the operating environments, data, processes, and storage. Identity, whether of the end user, vendor, application, process, or partner platform, is leveraged throughout this process, and as the span of the enterprise expands and becomes more complex, the more likely it is that one will use AI-type analysis to spot anomalies from expected behavior. These challenges are being addressed in policy, planning, operational, and standards bodies and include public-private collaborations such as the DHS ICT Supply Chain Risk Management Task Force and Alliance for Telecommunications Industry Solutions' 5G Supply Chain Security working group. Examples of capabilities and techniques being evaluated to enhance this visibility and risk management include ZTA, hardware and software bill of materials, root-of-trust based attestation, and micro-segmentation of operational services into encapsulated domains to reduce the opportunity for lateral movement of malicious behavior into other domains.

Since this class of incidents was exposed, NSTAC companies and their peers have been actively engaged with their U.S. Government partners to better understand the problem and develop solutions in a collaborative environment. While NSTAC's understanding of the threats and vulnerabilities facing the global supply chain is growing, many tools to increase the visibility and control of any given environment are moving into the adoption phase. Adopting these tools and strategies provides the opportunity for the U.S. Government to be actively engaged in the forums where capabilities are being defined. It also allows the U.S. Government to take the lead in procuring and adopting products and services that incorporate these security aspects, which should act as a further incentive to incorporate these capabilities into the broader ecosystem.

Non-Dependent Challenges

During a risk analysis of a large, complex ecosystem, some challenges are predictable and part of the natural variable set of things that can go wrong either because they are an opposing state of a normal function or because they present an inherent dependency created by the use of such a system. For example, equipment will fail, configuration mistakes will happen, adversaries will continue to subvert and attack systems. Similarly, more wireless and wireline densification requires more spectrum and more infrastructure; while they may be challenges, they are to be expected. Other challenges may not necessarily be directly tied to the system in use. While not unforeseen, they are also not predictable due lack of direct correlation to other variables within the system. For example, a certain technological impact may or may not occur regardless of its increased use or applicability in the ICT ecosystem.

Evolving Technological Threats

Advances in technology over the next decade across a wide breadth of disciplines will produce great benefits to ensure resilient communications networks and service delivery. These same technological advancements could also be exploited by adversaries and malicious hackers as cyberattack tools. Essentially, as new technologies are developed over time and without appropriate countermeasures, the potential exists for them to be utilized for the common good or harnessed for nefarious purposes. Examples of this are the following:

- IoT's expansion of the threat surface – The use of "smart" connected devices continues to permeate mainstream use cases, and, as more data gathering, automation, and remote capabilities are required, the number of these devices will grow exponentially. The massive scale of these devices, approaching tens of billions, increases the threat surface across the broad ICT ecosystem. IoT devices, in some cases, pose a higher security risk than classic IT endpoints (phones, laptops, desktops, servers, etc.) because they are often built to perform a specific function at the lowest possible cost with limited processing capacity and maximum battery life. Currently, many of these devices are not capable of supporting on board security, so alternative

countermeasures in the network or application of other security mitigations are required.

- AI and ML for smarter and more resistant malware, ransomware, and DDoS attacks – AI and ML technology will be used in the future to strengthen detection and mitigation defenses against novel and large-scale attacks. This same adaptability and speed will also be deployed by attackers to subvert and penetrate those defenses, creating attack scenarios that morph unexpectedly over time.
- Data poisoning to corrupt decisions produced by AI algorithms – The output of AI systems is dependent upon the data input to those systems and the collection of data of all kinds for use in learning, modeling, testing, and more is growing at a rapid pace. Data poisoning is the technique of corrupting data to produce inaccurate or untrustworthy outcomes, which can lead to faulty decisions, financial loss, or compromised safety. Increasing dependency on AI without adequate research into counter-adversarial techniques, data integrity, and attestation methods increases risks from data poisoning.
- Deep learning to produce deep fakes – Advances in AI technologies such as deep learning and neural networks will push the envelope for application development in commercial, educational, historical, and training services, among others. However, as these sensory technologies continue to advance, the sophistication of deep fake images, videos, and audio will progress as well, making it more difficult to discern a deep fake from an authentic representation, eroding trust in many transactional interactions and paving the way for new fraud activities.
- Compromise of foundational public key-based cryptography by quantum computers – Quantum computing promises many new innovations and efficiencies at some point in the future. However, the evolution of quantum computing will eventually enable Shor's algorithm to be utilized against asymmetric algorithms, breaking encryption for some of today's commonly used cipher suites and retroactively compromising encrypted copies of data protected by those cipher suites.
- Theft of biometric data compromising identity access management – Biometric data (something you are) is increasingly used in multi-factor authentication as an alternative to hard tokens (something you have) or passcodes (something you know). Since it is not changeable or replaceable, this data is at risk of theft to then be exploited by attackers to gain unauthorized access to sensitive information.
- Advanced fabrication techniques for semiconductor counterfeiting – The same technologies and techniques that improve semiconductor manufacturing efficiencies will be used by adversaries to build counterfeit chips that resemble and perform as well as the original. The increasing complexity of systems on a chip makes it easier to hide malicious functions, placing increased burden on securing the semiconductor supply chain.
- Software supply chain attacks compromising trust of digital signatures – The use of digital signatures to provide for attestation of integrity (among other uses) in hardware manufacturing and software development has been an important step in shoring up security of the supply chain. Multiple large-scale, impactful attacks over the course of 2020 and early 2021 have exposed new attack vectors through the supply chain of companies. The complex and software-driven nature of modern infrastructure requires a high level of due diligence and maturity in the area of Supply Chain Risk Management.

Despite the many positive benefits these technologies bring to the Nation, NSTAC recognizes that these same technologies can be exploited with malicious intent. While in no way diminishing the potential threat, these very issues are being actively addressed in numerous forums now, just as future threats will be addressed in new venues.

Technological Discoveries

As the world pushes toward new advances in science and communications, whether it is for the common good, market dominance, or other reasons, a few key areas may have a significant impact on ICT environments and disrupt the anticipated future state of ICT in 2030.

The Form of the Future Internet: New IP and Its Alternatives

Several efforts, including those at the IETF and International Telecommunications Union Telecommunication Standardization Sector (ITU-T), are ongoing to develop new architectures and, eventually, the standards and protocols for the next generation of today's internet protocol networks. The IETF, which manages the current TCP/IP protocols of today's internet, continues to develop new implementations and standards that extend and improve the TCP/IP stack. Current IETF efforts include work on new transport technology, security and privacy, IoT, and automated network management. In parallel, the ITU-T, through its focus group "Technologies for Network 2030," is developing "future network architecture, requirements, use cases, and capabilities of the networks for the year 2030 and beyond." The ITU-T focus group established use cases, such as holographic and tactile networking applications, supported by multiple distributed network edge sites to support extreme bandwidth and latency demands. At the same time, the focus group described a network architecture that would leverage artificial intelligence, machine learning, and neural networks to identify and locate malfunctions in the network.[49]

Companies from competing nations have used the ITU-T focus group to push their vision called New IP, which "introduces variable length addresses; reintroduces circuit-switched-like principles in what is dubbed 'better than best effort networking'; suggests an approach to enable packets to embed contracts to be enforced by intermediary network elements in a way that is reminiscent of active networks where packets contain code to be executed by routers and switches; and presents the concept of 'ManyNets' where instead of a single network, the Internet would become a patchwork of networks loosely interconnected via gateways." This New IP combines the capabilities of today's IP, referred to as IPv4 and IPv6, with new capabilities that inherently provide enhanced quality of service, security, and privacy at the cost of these capabilities having centralized surveillance and control, placing individual liberty at the mercy of a centralized authority.

While New IP is not yet a fully fleshed-out proposal, its core concepts are being actively championed by China and other countries in the ITU-T. Its top-down design, development, and implementation approach differ significantly from the IETF's practice methodology of developing environments and protocol standards in parallel. As a result, the experience gained with initial implementations and interoperability testing at internet scale rapidly feeds back into the development effort. This discontinuity from the current standards approach, combined with other Chinese economic and political initiatives designed to limit western influence, such as the Belt and Road Initiative, threaten to bifurcate future networks.[50]

It is critical that work toward future standards for tomorrow's IP networks be performed collaboratively and openly to ensure new standards work with the existing internet. Just as China has proposed its vision for what New IP should look like, so too should the United States and its allied partners develop a comparable vision and a strategy to ensure that the global benefits attained over the past 50 years are extended into the future. Ensuring a fair and open internet not hostile to U.S. interests will likely require a coordinated and focused U.S. presence within ITU-T and other standards organizations for the foreseeable future.

Evolutions in Secure Internet Routing

The greatest risk to internet security is the hijacking of routing and domain tables used to move information from point A to point B. Malicious hijacking is being used by adversaries to monitor and steal information. The two internet protocols with the greatest risk from hijacking or manipulation are Border Gateway Protocol (BGP) and Domain Name System (DNS). The IETF standardized security extensions for both protocols, known as BGPSec and Domain Name System Security Extensions (DNSSEC), to ensure the authenticity of protocol messages to prevent hijacking. However, the cost and complexity of these protocols have slowed adoption on the internet.

NIST, along with industry collaborators, has produced a guideline, SP 1800-14B, Protecting the Integrity of Internet Routing, which offers best practices and

[49]ITU-T, Focus Group on Technologies for Network 2030, https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx

lessons learned regarding implementation of Route Origin Validation (in lieu of route path validation in BGPSec), but this solution has its limitations and is still being researched. DNSSEC alternatives such as DNS over Transport Security Layer and DNS over HTTPS have emerged, as they both provide encryption rather than ID validation capabilities, but commercial implementation is still split among the three choices, along with "none of the above" as a primary default. Without harmonized approaches to these two key essential technologies, it is difficult to predict what the state of secure internet routing will be in 10 years – further research, prototyping, and standardization are needed, ultimately influencing the evolutionary path of the internet.

Spectrum

5G is driving the need for increased mobile backhaul capacity. Microwave supports capacity scenarios for both backhaul and fronthaul. Higher frequency bands, above 100GHz, will enable capacities in the 40Gbps range and ultra-low latency over distances of about one-half mile. The 100GHz spectrum will free congestion at lower frequencies, enhance communications resiliency with new redundancy models, and enable new use cases for the industrial IoT and public safety. Technologies are being investigated and regulatory studies are examining deployment scenarios in the 92-114.5GHz and 130-174.7GHz frequency ranges, commonly referred to as the W-band and the D-band, for microwave backhaul. 6G will also drive future research in the THz frequency bands, 300GHz to 10THz. Given the variability of use cases, market guidance, and physical antenna and energy advancements, the modeling for usable spectrum in the future could take many different forms. Each direction(s) of research could shape the ability to drive any, all, or none of the benefits of higher speeds, lower latencies, broader coverage, or reduced power consumption.

Global Market Destabilization

Large economic powers within the global marketplace share interdependencies in common communications principles and protocols, a global market supply that benefits from scale and redundancies and mutual investment into the process of standardizing and building out the next innovation cycle. Destabilization can occur when one or more of these areas becomes heavily weighted or even split, creating multiple ecosystems that may drain resources, stagnate growth, or influence power struggles in other unforeseen ways.

Internet Bifurcation

China's Digital Silk Road (DSR) development program, within its Belt and Road Initiative, has become the platform for exporting Chinese technology throughout Asia, Africa, South America, and parts of Europe with the goal of building a global digital ecosystem that places China in control of information. The DSR provides a software-defined, virtualized substrate that enables China and its technology vendors to become the de facto standard internet infrastructure. The result is an increasingly bifurcated internet with a Digital Iron Curtain separating two sets of global hyperscaler cloud providers: those based in the United States and those based in China. The bifurcation will extend to geopolitical ideals and business ecosystems because the two sides of the Digital Iron Curtain have different world views on global economics, ethics, and human rights.

Because of its scale and advancements in the extensibility and performance of SDN/NFV, China can move forward in this direction with or without the realization and adoption of New IP proposals. Such a move would effectively bifurcate the internet due to technology selection and market dynamics, not just because of differences in routing architecture and approach. The United States and its allies need to have a bold vision for the future of the

[50]Clancy, Charles, MITRE, "Internet Futures: Challenges and Opportunities" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 3, 2020)

internet and lead its global realization through multi-lateral collaboration. Internet technologies should be specified in open standards bodies, including the IETF, that form consensus-based decisions based upon technical merit to implement a shared vision that maintains a singular open and interoperable global internet.

Supply Chain-Based Global Economy

A competitive marketplace and vendor diversity in the global communications network supply chain are important to the economic security of the United States. These national interests are undermined when companies backed by nation-states attempt to squeeze out competitors and dramatically expand their market share as part of a deliberate strategy. For example, Huawei has received as much as $75 billion in support from the Chinese government,[51] which has led to the company growing immensely during a time of significant market consolidation in the supply chain of radio access technologies for communications networks. If these trends continue, the geopolitical and economic posture of the United States, as well as the resiliency of its communications infrastructure, could be adversely affected.

Creating an environment to foster competitive, vibrant, and trusted suppliers is not a challenge that can be addressed solely through unilateral action by the United States. Competitiveness in the communications equipment market requires economies of scale, and the U.S. market by itself is not sufficiently large to achieve the goal of a level economic playing field. Progress in this space will therefore require coordination among the governments of multiple like-minded countries.

Standards

Standards bodies with a consensus-based approach to establishing specifications based upon technical merit have produced open and interoperable technological solutions benefiting the global community. It is critical that standards bodies do not transition toward a top-down model in which a government can influence decisions and specifications based upon its national interests. The U.S. Government, its allies, and private industry should continue to collaborate in international standards bodies to establish technical merit for critical technologies that impact national security but may gain gradual commercial interest through the next decade. Attention to standardization of technologies including quantum cryptography, quantum computing, AI/ML, blockchain, and high frequency applications will ensure fair and balanced use when markets are ready. It is also in national interests that NIST and CISA continue to provide guidance for industry best practices of key technology enablers including DevSecOps, secure use of open-source software, ZTAs, supply chain risk management, and secure operational configurations.

Summary of Findings and Analysis of the Future State of ICT

Over the course of the resilience study, a recurring set of critical precursors—activities, capabilities, and resources—emerged that often cut across subsectors. These foundational elements must be in place to deliver the desired security and resilience outcomes in future communications networks.

Network Densification and Ubiquitous Connectivity

Communications sectors are building toward ever more dense and capable networks to deliver many end capabilities – not only security and greater reliability, but also economic benefits that will enable future networks to run profitably enough to continue further investment in growth and innovation. Ubiquity of networks will need to go beyond basic connectivity; it must meet rigorous expectations for bandwidth, latency, ease of use, flexibility, and resilience. Further, the densified layers are expected to mesh together in ways that allow a range of redundant connectivity options for end devices and enterprises.

Wireline networks will be a significant part of the densification. Fiber to the home will increasingly become the norm wherever population density supports it. Even in remote areas, where wireless networks shoulder more of the last mile of connectivity, robust fiber networks will provide the backhaul and aggregation of exponentially increasing traffic from homes, businesses, and other

[51]Chuin-Wei Yap, Wall Street Journal, "State Support Helped Fuel Huawei's Global Rise," December 25, 2019, State Support Helped Fuel Huawei's Global Rise - WSJ

networked devices. National and global wireline networks will follow the same path, with meshed and redundant fiber networks offered by both traditional carriers and hyperscalers delivering extremely high data rates through an interconnected and resilient internet backbone. Undersea cable infrastructure will continue to grow, with an expectation that alternative routes will mitigate potential risks from concentrated cable routes and landing areas. To deliver these various connections, providers will need physical access to rights of way along aerial, underground, and undersea corridors.

In parallel, current and future iterations of cellular and Wi-Fi networking will deliver ever more dense and capable wireless connectivity for individual users, exponentially increasing the number of IoT devices and sensors. These future wireless networks will be delivered by a range of appropriately sited base stations and access points based on the connectivity needs of the connected devices. Satellite, land mobile radio, and microwave connectivity will complement terrestrial wireline and cellular wireless networks to round out near-universal availability of highly capable networks. Future generations of small, inexpensive satellites in a variety of orbital constellations will provide broadly available data connectivity for a wide range of end users. Public safety and other land mobile radio users will operate resilient LMR networks that mesh intelligently with cellular and satellite systems and are powered by robust fiber optic backhaul. The expansion, availability, and predictable policy appropriation of the usable spectrum will be critical to delivering these more dense and resilient wireless networks. At the same time, support for placement of physical infrastructure (base stations, fiber conduit, undersea cables, orbital assets) must be properly anticipated, managed, and streamlined across federal, state, and local levels.

The evolution from 5G to 6G will be dependent upon a number of technologies that are expected to rapidly advance through the decade. Software applications in the cloud are evolving from virtual machines running a guest operating system on top of virtualized hardware to cloud-native microservices that run-in containers on top of a virtual operating system, reducing overhead while increasing portability for more agile cloud services. The cloudification of the network and practical deployment experience will produce cloud-native applications that achieve the quality and security of today's telecom service providers, while advances in software and network architectures enhance network automation, orchestration, and elasticity. Real-time network monitoring will measure KQIs and security to help provide automated adjustments to network slice resources and configurations so that slice-specific quality and security requirements for 6G use cases are met. All these technologies will use AI for automated real-time decision-making. Advances in active hardware components, including semiconductor fabrication and massive MU-MIMO antennas, will enable the network to meet the scale and performance required for 6G use cases, many of which will be dependent upon mmWave, 100Ghz, and THz frequency spectrums. The network of the future will be built upon a foundation of DevSecOps development processes using continuous integration/ continuous delivery and open, interoperable trusted international standards.

Incorporation of the Enterprise into Shared Risk Planning

Leveraging edge and cloud environments along with ubiquitous connectivity will enable enterprise-specific platforms to deploy applications faster, dynamically, and more efficiently. At the same time, the integration of enterprise networks, applications, and compute options will add tremendous complexity to security environments. To avoid giving an attacker an advantage, the market will need to learn lessons from cloud adoption and embrace a shared risk responsibility and a security-first mentality. The United States recently moved from a Cloud First to a Cloud Smart approach. Cloud First granted agencies broad authority to adopt cloud-based solutions. Cloud Smart offers practical implementation guidance for Government missions to actualize potential of cloud-based technologies while ensuring thoughtful execution that incorporates practical realities.[52] The U.S. Government can adopt a similar "Smart" approach for new technologies that incorporates appropriate security guidance, driving adoption and pushing those best practices further down into the enterprise sector.

As enterprises leverage a multitude of platforms and rely on that infrastructure to execute their mission, it will be essential to build in holistic security throughout the network to reduce exposure and mitigate risk from

new and emerging threats. Taking advantage of the resiliency and operational benefits of the underlying ICT infrastructure will require developers, users, and service providers to partner and operate within the ecosystem of trusted vendors/providers chosen and customized for that enterprise.

Reliance on Cloud-Based Services

While public cloud providers address security and resiliency throughout their architectures, it remains difficult to measure the reliability and security of the cloud. Across the globe, nations are considering new policies to address their dependency on large public cloud providers, especially as their adoption of providers of critical functions grows. The policy goals seek to enhance cloud provider security and resilience and better understand core dependencies and risks. In the People's Republic of China, for example, policymakers are leveraging ICT industrial policies to increase the visibility of interdependencies in their ICT infrastructure to enhance national resiliency. Meanwhile, the European Union is revising the Directive of Security of Network and Information Systems to include proposals to consider cloud providers essential entities.[53] In Australia, efforts are underway to define cloud providers as critical infrastructure, given their underpinning of Australia's digital economy.[54]

Three separate opportunities exist to enhance cloud resiliency in the context of potential systemic weaknesses and concentration of risk for other sectors dependent on the cloud. The first is understanding collective cloud risk better through formal research on customer usage, universal cloud dependencies (e.g., potentially PNT), risk concentration, and resiliency assessments. The second is increasing transparency for how cloud providers mitigate risks. Doing so should involve a renewed focus on standards as a tool to enhance visibility into cloud dependencies and mitigations while reducing cross industry complexity, as compared to more prescriptive technical requirements that could ultimately hinder innovation. For example, existing audit and cybersecurity standards in use by cloud providers today could be augmented. The third opportunity is to align the security and resiliency investments made by cloud providers and customers to positively reinforce each other by: (a) decreasing the security knowledge gap and better defining security responsibilities between providers and customers; (b) increasing guidance to help customers assess their risk appetite and implement mitigation strategies; and (c) developing SaaS approaches so provider and customer contingency plans are complementary, coordinated, and inclusive of dependencies and they appropriately address the responsibilities of each party.

Secure and Resilient Supply Chains

This study repeatedly highlighted the need for secure, reliable, and resilient hardware and software to run future networks. Hardware supply chains must be secure and reliable, down to the precursor materials, such as rare earth minerals, necessary to produce networking devices and equipment. The supply chains that deliver these products should be as geographically diverse as possible to minimize the risk of disruption due to political instability, trade disputes, natural disaster, or pandemic. As discussed in depth earlier, chip design and manufacturing must be carefully managed to ensure critical applications have the appropriate security built in. Software supply chains must be similarly secure while maintaining the benefits of global production and open-source code. As software overwhelmingly takes over network management and control, service providers must be confident in both their control software and the underlying machines that process it.

A long-term strategy for the Nation's ICT supply chain should be built upon the foundation of security, integrity, and resilience. Supply chain integrity and the availability of the right component at the right time, delivered in a secure way, will become essential to business. Over the past few years, several large ICT vendors and operators proactively executed a regionalization strategy for their supply chains by

[52]Cloud Smart, "From Cloud First to Cloud Smart," 2021, https://cloud.cio.gov/strategy/

[53]European Union Agency for Cybersecurity, "Network and Information Security Directive," July 2016, https://www.enisa.europa.eu/topics/nis-directive

[54]Australian Government Department of Home Affairs, Critical Infrastructure Center, "Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Document," November 2020, https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf

placing manufacturing and development as close to the customer as possible in order to mitigate potential risks or regional disruptions and reduce dependence on one supply site or vendor. Doing so allowed the communications sector to mitigate many of the supply chain disruptions experienced in other sectors of the United States during COVID-19.

The Broad Impact of Quantum-Based Technologies

Upon review of emerging technologies that can help build a more resilient infrastructure, NSTAC was encouraged by the advancements in practical quantum computing and its ability to handle government scale priorities. It should be noted that similar efforts are underway by adversaries and allies alike. This provides both an opportunity, in commonality of effort and increased efficiencies of scale, and a threat to the United States in that adoption and mastery of these domains may provide a significant adversarial advantage that cannot be overcome. The National Quantum Initiative Act (Public Law 115 368) was signed into law on December 21, 2018. Its purpose was to ensure the continued leadership of the United States in quantum information science and its technological applications. Congress intended for it to be inclusive of all available and viable technologies and develop near-term applications as well as long-term research and development projects.

Activities associated with this Act, such as the Department of Energy's efforts in the areas of education and training, are already underway.[55] Nonetheless, it is not clear if all aspects of the quantum life cycle are being addressed equally. NSTAC recommends that the U.S. Government contract with a federally funded research and development center to create and manage a quantum "sandbox" that could serve as a testbed for the near term Government quantum application development and testing. NSTAC also recommends that one focus of this effort include addressing next-generation network problem sets highlighted within this report.

NIST is currently working with the international cryptographic community to develop and select quantum-resistant public-key cryptographic algorithms to protect network communications and data at rest. Selecting the algorithms is just the first step. Nationwide deployment of the selected algorithms will be a major endeavor. NIST has stated in the past that the average cryptographic transition is nearly 15 years. With the potential national security implications of having existing, at-rest data exposed at some point in the future, it is vital that the Nation begin a transition and deployment as soon as feasibly possible. This transition will require mobilizing communications technology and protocol providers to integrate these Post Quantum Cryptography (PQC) algorithms into the underlying communications and into select open-source projects (such as OpenSSL). Encouraging or even incentivizing adoption of selected algorithms into their products' encryption capabilities is also necessary. Reducing the transition time needed for adoption and deployment requires an effort to plan and manage the research and integration of selected PQC algorithms.

The United States must encourage skills development, fund research, and enhance coordination among public, academic, and commercial efforts to meet the goals of the Nation. Quantum computing promises greater advances in efficiency for the end user experience thanks to optimizations in real time achieved in areas such as improvements in supply chain management (route planning, inventory optimization), network capacity optimization (resource utilization), network resiliency and cybersecurity, and manufacturing optimization (staffing, factory automation). Quantum communications and quantum encryption promise enhanced security for end-user applications such as electronic communication, financial transactions, telemedicine, and commerce. Quantum computing promises great efficiency advances, and quantum encryption and key generation promise great security advances. Quantum communications for key exchange between two endpoints should provide a basis for optimally secure and resilient communications by the end of this decade.[56]

[55]National Quantum Coordination Office, "DOE Quantum Research Center Announces Quantum Computing Summer School," March 30, 2021, https://www.quantum.gov/doe-quantum-research-center-announces-quantum-computing-summer-school/

Accelerating Artificial Intelligence Implementation

Artificial intelligence is already a fixture in many aspects of modern communications networks, but as networks become ever more software driven and self-adjusting, the security and resilience of AI implementation will become fundamental to the security and resilience of the overall networks. AI powered cybersecurity systems must have access to quality pools of training data and must evolve quickly to help human and automated threat detection and mitigation, while also learning to detect and counter attempts to confuse or "poison" its learning models. Both AI and human network defenders will need to adapt to and counter adversarial use of AI to target U.S. networks and infrastructure.

To accelerate the AI competitiveness of the United States, the National Security Commission on Artificial Intelligence's recommendations include substantively increasing non-defense R&D investment annually, establishing new AI research institutes, supporting a national-scale testbed and open network infrastructure, collecting and making available large-scale open training data, and undertaking significant work with international coalitions to create "a favorable international AI order."[57]

Finally, note that data – representative data of all imaginable types, in massive amounts – is critical to the ability to create effective AI solutions with integrity. Preserving access by U.S. industry and the Federal Government to such stores of data should be thought of as a new critical infrastructure challenge, where the data itself is the critical resource. Similarly, bidirectional sharing of trustworthy, actionable operational and performance intelligence should be supported by harmonized schema and aligned static and AI-driven data sets. National efforts to build AI/ML models for network optimization and anomaly detection will be needed, given the broad set of data required for automation and orchestration across critical infrastructure.

Standards and Interoperability

Interconnection is in many ways the fundamental purpose of a network; therefore, standards are crucial to the security, the resilience, and even the basic operation of communications systems. As technological development continually expands the art of the possible, it is crucial that standards develop and evolve apace, and that those standards do not unduly impact the Nation's ability to compete in the global marketplace or adversely impact the security and resilience of the United States and its communications systems. Across a variety of contexts and ranging from voluntary "consensus" standards to broad, more formal global arrangements, the United States must recapture leadership in the arenas where standards are set so as to preclude peer competitors from using international standards to hinder or even threaten U.S. interests.

Resilient and Ubiquitous PNT Services

PNT systems are fundamental to modern communications networks. The U.S. Global Positioning System has long provided the foundation of PNT services and has recently been augmented by other space-based constellations operated by allies and adversaries alike. As networks densify and approach "ubiquitous coverage," PNT services will be necessary in places where space-based alternatives are unavailable or unreliable, such as in urban canyons, inside large facilities, underground, and under the sea. Further, given the reliance of communications systems and other critical infrastructure on PNT and the threats to PNT resilience from space weather, jamming, and even anti-satellite weaponry, PNT assurance would be greatly improved with the addition of terrestrial backup capability.

Power Remains a Key Dependency

The power and ICT sectors share mutual dependencies. Work is underway within DHS' National Risk Management Center (NRMC) to better understand the dependency and interdependency of cross-sector critical functions. Meanwhile, a closer and more

[56]Vermeer, Michael, RAND, "Securing Communications in the Quantum Computing Age," 2020, https://www.rand.org/pubs/research_reports/RR3102.html

[57]National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

focused future assessment of how these sectors can plan now to assure more resilient future outcomes could drive automated or sensor aware solutions while each sector is in these early stages of this evolution.

The consequence to ICT for any long-term power outage can be largely mitigated, however, if there is fuel available to sustain the sector's back-up generators.[58] Plans to mitigate this contingency can be made, but further work to understand the quantity of stockpiled fuel available and whether entities providing critical functions could have access to this fuel and under what circumstances is still needed.

ICT Is an Integral Component of National Security

As President Biden notes in his Interim National Security Strategic Guidance, the concurrent revolutions in technology, such as those discussed above, offer both "peril and promise": "The world's leading powers are racing to develop and deploy emerging technologies, such as artificial intelligence and quantum computing, that could shape everything from the economic and military balance among states to the future of work, wealth, and inequality within them."[59] Within this geopolitical context, the Nation's security strategy lays out a framework to help protect the security of the American people, expand economic prosperity and opportunity, and defend the democratic values at the heart of American life.

The ability to hyper-connect millions of devices and sensors will fundamentally transform the future military and security environment. The robust and resilient networks and technologies described earlier in this section will create capabilities that DoD and the intelligence community can harness through technology adoption or contracted services. Outside of traditional military and security contexts, ICT companies are a critical part of international civil society engagement on a range of technology and cybersecurity issues. It is necessary to work alongside like-minded partners to uphold existing and shape new global norms in cyberspace, and this work will become even more critical as new paradigms for the structure of the internet evolve and take hold.

At the same time, the centrality of these future hyperconnected networks to national defense and the Nation's economic vibrancy may also make them targets for determined adversaries. Communications providers already play the critical role in defending their own networks and identifying, mitigating, and countering malefactors—nation-states and cyber criminals—who seek to target those networks and systems. However, determined, well-resourced, and highly technical nation-state adversaries have repeatedly demonstrated their intent to target the networks, software, and supply chains that enable the Nation's communications. Countering nation-state adversaries is properly the sphere of the national defense establishment, so it will remain critical that communications providers and the Nation's cyber defense team collaborate in those closely intertwined areas of responsibility. Information sharing, most likely on a machine-to-machine basis, will become critical, so that network operators can be alerted to threats, particularly through identification of anomalous behavior.

ICT also furthers national resiliency by helping to stabilize and reduce human suffering in communities impacted by disasters, enabling rapid collection and ingestion of data to deliver greater situational awareness and propel data-driven decisions when and where they are most needed. ICT then provides the means to communicate these decisions to responders and the public across denser, more resilient, and more capable networks that will help ensure those messages reach their target audiences in rich and detailed voice, graphic, video, and tactile formats to facilitate action in crisis.

The coming era of hyperconnectivity will leverage the same technologies that ushered in "work from anywhere" during COVID-19 to enable "respond from anywhere" during disasters, offering great flexibility in crisis response, but this connectedness also brings challenges. Cybersecurity regulation is intended for normal situations, but it often constrains complex disaster response missions. Unique privacy, IP, and security laws differ widely across jurisdictions,

[58]National Defense University, "Severe Space Weather Threats: National Electrical Grid and Impacts to Critical Infrastructures – After Action Report," 2011

[59]"Renewing America's Advantages - Interim National Security Strategic Guidance," The White House, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

complicating a "respond from anywhere" approach. In the past, it was possible to cordon off a physical area to prevent outside malefactors from interfering in the disaster response and recovery, but today's opportunists can also launch "scam from anywhere" to take advantage of a crisis situation.

Policy makers at local, state, regional, and national levels around the world need to address the ways that ICT has shifted the response landscape. Remote response could be facilitated through a standardized process for exceptions to certain privacy, data, and cybersecurity regulations during disasters. Such a process would be similar to the Special Temporary Authority granted for spectrum use or disaster network management processes. In addition, the private sector in the United States is subject to federal and state laws that control its ability to give services and resources freely to federal and local response agencies. Adding authorities into standardized emergency declarations that enable the provision of remote response contributions while providing regulatory flexibility would help realize the potential of ICT enabled disaster response.

ICT also provides an economic engine to spur innovation across the United States. As ICT companies develop, implement, and master new technologies, they produce the economic benefits that fund the next round of new technology. At the same time, these developments deliver capabilities, including security and resilience, that will permeate across all infrastructure sectors, the defense establishment, other businesses, and consumers. As such, the capabilities built into the current and future networks can provide for a level of economic and societal resilience to keep the Nation's economy vibrant and productive even in the face of disruptions up to and including a worldwide pandemic.

One of the key components of ICT's economic framework is the development and leveraging of critical global supply chains for hardware and software. Other nations, economies, and enterprises seek to emulate the U.S. model that leverages the global economy to source goods and services where they can be produced most efficiently and securely. At the same time, this supply chain includes risks that must be managed. Any overreliance on single nations or regions for essential goods and services can raise vulnerabilities to physical disruption or adversary weaponization of critical supply chains. At the most fundamental level, the Nation should strive to understand to what extent it can rely on the secure provision of goods and services in a highly stressed environment. Where the security or assured provision of critical goods and materials is at too great a risk, the Nation should develop incentives to restore domestic production capacity.

As identified in the Cyberspace Solarium Commission report[60] and recently directed under the 2021 National Defense Authorization Act,[61] the United States must secure this economic advantage through creation of a Continuity of the Economy plan. Using the set of National Critical Functions as its central organizing principal, the plan will address risks, including those across multiple sectors, resulting from future disruptive events. The Administration should continue to gain a deeper understanding of the National Critical Functions, not only at the subfunction level, but also with the goal of gaining a deeper understanding of the assets, components, and systems that are necessary for their routine functioning.

Finally, for the Nation to maintain its global strategic technological and economic advantage over the coming decades, its educational system must continue to provide workers with the skills necessary to keep up with the advancing pace of technology and digitalization of the economy. As the COVID-19 pandemic has shown, the skills of a majority of the workforce have had to undergo a rapid evolution so that the economy can continue to operate in a remote work environment. While these challenges were overcome in some sectors thanks to proactive investment and planning, the United States will need to build out its workforce so that it can be rapidly deployed to address new challenges and ensure that the tools and necessary training can be rapidly integrated.

NSTAC recognizes that there are challenges associated with moving to this next generation of interconnectivity and is actively engaged in addressing and resolving these issues – most notably, the whole-of-Government analysis of what mitigations need to be in place to assure a trusted supply chain.

The Nation is at an inflection point where its strategic actions and long-term planning now will have a significant impact on its ability to maintain its global leadership position over the next decade. The seventh edition of the National Intelligence Council's Global Trends report outlines five future scenarios, three of which have direct relevance to this report: Renaissance of Democracies, Competitive Coexistence, and Separate Silos.[62] NSTAC contends that actions taken now will better position the Nation to lead the technological achievements outlined in the Renaissance scenario, to retain its competitiveness in the Coexistence scenario, and create a resilient, self-sufficient economy should the Separate Silos scenario come to fruition. This report reiterates the conclusion made previously and contends that "while the full impact of interrelated technology developments is not foreseeable, many potential opportunities and risks can be anticipated; in particular, the Government's NS/EP functions will likely be both enabled and challenged by forthcoming technology developments. As such… the Government must harvest the significant NS/EP benefits of forthcoming technology while also addressing new threats and vulnerabilities."[63] The recommendations in the next section reflect activities that require new or continued planning or actions to prepare for this future in time to capitalize on it.

Summary of Actions the Administration Can Take to Support the Future ICT Vision

Public/Private Planning, Consultation, and Risk Assessments

The hyperconnected environment of the future will necessitate a higher level of consultation and collaboration between industry and Government to address future challenges. NSTAC notes that public/private planning has been highly successful in the ICT sector and should be retained as the preferred means to address difficult or challenging issues. There are six key opportunities for improvement that the Administration should focus on to achieve the key objectives outlined throughout this report.

Changes in Emergency Preparedness Practices/Procedures

The nature of response required in these evolving networks, as well as who will be responding, needs to be considered. If incident response is being provided remotely, federal and state disaster declarations may need to be more uniform to empower private sector responders to freely assist response agencies and victims by modifying procurement rules and potentially other cybersecurity regulations during emergency response. For instance, during declared emergencies, limitations on data usage, privacy protections, etc. may need to evolve. As such NSTAC reiterates an earlier recommendation:

> The Government should assess the communications infrastructure leveraged in an emergency – including users/devices, the customer edge, access, the core, IP services, and applications/content – and determine whether relevant stakeholders have been identified and/or included within NS/EP public-private partnerships, ensuring that coordination and agility are realized in advance of an NS/EP event. It must also plan for response events that require the assistance of critical organizations that were not identified in advance and are not part of any existing public-private partnership. In doing these activities, the Government should recognize that application and content providers, including social media, messaging applications, and AI applications, are increasingly leveraged during an emergency.[64]

Communicating the Resiliency of Underlying Cloud/Edge Environments

As the U.S. Government and private enterprises begin leveraging the capabilities of commercial access, edge, and cloud providers upon whom they will rely, an effort

[60]Gallagher, Mike and King, Angus, "Cyberspace Solarium Commission," March 2020, https://www.fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf

[61]United States Congress Government, "Fiscal Year 2021 National Defense Authorization Act," January 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395/text

[62]Office of the Director of National Intelligence, Global Trends 2040, https://www.dni.gov/index.php/global-trends-home

should be undertaken to communicate the security, resilience, dependencies, and supply chain practices of these platforms. Aspects incorporated into these communications will likely involve communicating the underlying hardware, software, and partners leveraged, which in turn can be developed to represent a trust environment for the enterprise, based on unique risk-based considerations.

Impact of Geopolitical Issues

The future hyperconnected environment lends itself to more frequent and integrated consultation on policies developed. In particular, the U.S. Government should consult with industry on two emerging topics:

1. Given the geopolitical threats to the supply chain, continuous assessment is necessary to determine whether and how to adapt supply chains to mitigate or counter conflict-based supply chain disruptions, such as compromise, reduced availability, or increased demand.
2. Investigate how to integrate, live with, or otherwise address the potential geopolitical fragmentation of the global supply chain.

Forward Assessment of ICT/Power Dependencies

Given the reliance of the Nation on the critical functions provided by the communications, IT, and power sectors, NSTAC recommends that National Security Council – Resiliency Staff act as the sponsor for a forward-looking analysis of how the dependencies among power, IT, and communications will change, and what opportunities exist to operationally interact or inform each other to mutually assure the delivery of each sector's critical functions. Work within the DHS NRMC is already underway to better understand the dependency and interdependency of cross-sector critical functions. Therefore, collaborating now to assure future outcomes could drive more automated or sensor-aware solutions and mutually assure each other's services while each sector is still in early stages of this evolution.

Continued Reliance on Fuel: Stockpile Issue

Most post-event consequences of an LTO to communications and other sectors can be mitigated if there are sufficient reserves of fuel (diesel, gasoline, propane, and potentially in the future, alternative sources such as hydrogen fuel cell and battery). Since fuel reserves are controlled at both state and federal levels, it is critical to understand how much fuel is available and whether some portion should be held in reserve to support critical functions. In the interest of large-scale response planning, NSTAC recommends that a study be conducted to assess the following:

- How much fuel does the Nation have in state/federal fuel stockpiles at any given time?
- If there are X million gallons of fuel, how long would that fuel sustain the essential services for a state, a region, or the Nation?
- Under what circumstances could ICT providers (or critical infrastructure operators) get access to that fuel?

Next Generation IP Strategy

- The U.S. Government should develop a whole-of-Nation strategy, including allies, to ensure the next generation Internet Protocol is developed in an open, transparent, industry-led environment that includes academic think tanks and research.
- Develop a United States/allied vision (with industry) to guide the secure expansion of the internet into the next decade and beyond. This vision should reflect the evolution necessary to accommodate changes in technologies as well as the SDN/NFV and cloud-native environment but should also be developed with an eye to minimizing the risk of a bifurcated internet landscape.
- Engage with allies in standards groups to reinforce approaches to technology development, application, deployment, and intellectual property protections that are aligned with the strategic goals of the Nation.

[63]National Security and Telecommunications Advisory Committee, "NSTAC Report to the President on Emerging Technologies Strategic Vision," July 2017, https://www.cisa.gov/publication/2017-nstac-publications

[64]National Security and Telecommunications Advisory Committee, "NSTAC Report to the President on Emerging Technologies Strategic Vision," July 2017, https://www.cisa.gov/publication/2017-nstac-publications

Recommendations to Support Deployment of Future Networks

The following recommendations highlight areas for continued attention to ensure the ICT ecosystem is built out expeditiously. The White House should consider the national economic and resiliency benefits associated with the extension of next generation networks and supporting infrastructure as an integral part of any Administration infrastructure proposals. Policymakers should also consider how building out the system may result in increased national resilience to physical or cyber incidents, including where a Continuity of Government or Continuity of the Economy plan would be activated.

Trusted Semiconductor Supply Chain

It is necessary to preserve the ability of the Nation's industry to continue to manufacture processors that are unquestionably trustworthy and beyond the reach of adversaries' ability to compromise their design or fabrication.

NSTAC therefore recommends:

- Supporting investments specifically for trusted foundries for high-assurance fabrication of microelectronics for use in the most critical applications and, generally, for increased onshore capacity for advanced manufacturing of microelectronics.
- Supporting the development of industrial standards for assured design, manufacturing, and packaging, in order to expand the number of trusted suppliers for equipment used in support of the National Critical Functions.
- Investing in research and development of technologies and techniques that would enable the Government to have more trust in processors and microelectronic technologies designed domestically but manufactured outside the United States. The research should include recognition and adoption of a hardware-based chain of trust, secure manufacturing facilities, and attestation/assurance mechanisms.
- Taking steps to ensure access to critical raw materials such as rare earth metals and other elements used in group III-V semiconductors. Ensure that the implementation of Executive Order 14017, *America's Supply Chains*, signed February 24, 2021, includes steps to protect continued access to these critical materials while also pursuing agreements with allies to secure alternative sources for these materials.

The recently proposed CHIPS Act is a first step in ensuring the availability of a trusted semiconductor supply chain.

Spectrum Policies

Spectrum is the key to rolling out next generation technologies for all forms of wireless. Expedited effort, coordinated by the National Telecommunications and Information Administration with industry input, is needed to adapt, update, and streamline national spectrum policies to provide sufficient spectrum for emerging use cases, and incorporate spectrum allocation and sharing for various new bands and mission spaces. An updated policy will provide immediate benefits for product development, consistent application of software-defined networking/artificial intelligence models as they relate to spectrum issues and accelerate closing gaps in coverage and service.

Fiber Deployment

Wireline fiber growth enables, and is driven by, wireless, edge, and cloud technologies. The Administration should seek to include underground and undersea fiber infrastructure projects as part of any new infrastructure package. In addition, other infrastructure projects such as bridges, pipelines, railways, port facilities, and highways, should incorporate support for fiber conduit as they are developed and implemented.

National Timing Architecture

Consistent with the National Timing Resilience and Security Act, and to assure market initiatives for the deployment of an alternative source of U.S. time, the Administration should develop a National Timing Architecture. Further, to enhance the ability of commercial entities to afford leveraging this architecture, the Administration should appropriate sufficient funds to lay the foundation, with the Federal Government being the first customer for what will ultimately become an interconnected, resilient PNT delivery mechanism.

Recommendations to Support Adoption of Key Technologies

The U.S. Government Can Foster Enterprise Adoption of Next-Gen Technologies

The 2017 *NSTAC Report to the President on Emerging Technologies Strategic Vision* noted that "In this environment, maintaining the status quo is inadequate and unacceptable. The Government must act with unprecedented speed and rigor… making fiscal and regulatory commitments that enable upgrades in technology and utilizing security models that improve governance and operational efficiency." The following recommendations focus on what steps the U.S. Government should be undertaking now to glean the resiliency and management benefits of new architecture and technology. Taking these steps will drive the necessary scale to encourage adoption across the enterprise landscape as well.

Adopting Enterprise Architecture Best Practices for U.S. Government Networks

- Review existing legacy systems and their operations, focusing on modernizing and replacing them with systems more efficient and easier to protect.
- Incorporate cloud and edge computing as part of the U.S. Government's network architecture and communications infrastructure resiliency planning.
- Leverage cloud service providers' security best practices (e.g., containerization of microservices, separation of concerns, independent testing, and certification) when developing enterprise and edge network technologies.
- Assure the integrity and quality of network components that support the National Critical Functions through certification labs and standardized practices.
- Use the full capabilities of SDN/NFV orchestration, supported by AI technologies, to automate the process of dynamic response to changing environments.

Cybersecurity Considerations for U.S. Government Networks

- Proactively ensure strong cyber hygiene by adopting cybersecurity best practices including risk based vulnerability management, ZTAs, signature-based defenses, and maintaining robust firewalls.
- To assure detection, mitigation, and incident response capabilities, maintain a robust asset management system, extensive access system logs, and security analytics to allow post-incident responders to identify, isolate, and remediate the damage from software supply chain attacks as quickly as possible.
- Develop or leverage commercially developed automated threat prevention technologies to assess and quarantine questionable system behavior at the endpoint and network level.

Standards

- The Government should prioritize and sufficiently resource agency participation in global ICT and cybersecurity standards forums to increase trust, transparency, and predictability for technology providers and users, including the government.
- The Government should develop mechanisms for regular collaboration with the private sector and other governments, enabling strategic prioritization and planning for standards development in strategic technologies.[65]
- The Government should support industry engagement in global Standards Development Organizations (e.g., Third Generation Partnership

Project [3GPP], Institute of Electrical and Electronics Engineers [IEEE], IETF, ISO/IEC) to assure industry forums remain the venue for standards development. Separately, the Government needs to be engaged in nation-state forums such as the ITU to protect national interests. Key areas for international standards engagement include:

  - Secure development processes, including standards for secure coding practices, cataloging methodologies, and integrity verification; these should be equally applicable to open-source software where it is ingested and used.
  - 6G wireless communication
  - Quantum computing and quantum encryption
  - Artificial intelligence
  - Interoperable APIs, interfaces, and functions for network, orchestration, and applications across all carrier, edge, and cloud models to facilitate the development of enhanced applications and network solutions.

- Zero-trust architecture will continue to be developed, enhanced, and further integrated into Next-Gen networks in the future, as evidenced by multiple briefings and study materials citing the need for such deployments as the next level of security advancement required for critical infrastructure. Government adoption and increased efforts in two key areas will ensure that the United States is in a position to define and shape the use of this technology.
- The Government should develop a consensus definition for zero-trust architecture, building upon NIST's National Cybersecurity Center of Excellence work and promoting this approach with other allied nations to ensure these concepts are adopted and rapidly built into all aspects of the ecosystem.
- The Government should conduct further development to ensure that mechanisms for federated entity identification are accommodated in this architecture.

Post Quantum Cryptography

Previous NSTAC reports—such as *Report to the President on a Cybersecurity Moonshot*—suggested there will be substantial global research and development around quantum computing, communications, and quantum-resistant cryptography over the next decade. Key initiatives that should be organized and incentivized by the Federal Government include:

- Develop a national strategy for cyber resilience on critical systems and sensitive communications, built around the National Critical Functions, that includes cryptographic agility in future systems (i.e., adaptability to PQC algorithms). Future risks introduced by quantum computing to then current systems as well as retroactive risks to now-current systems should be considered as well.
- Develop a post-quantum cryptography transition framework for Government systems that evaluates legacy systems, catalogs and analyzes the risk of public-key cryptography in use for various classes of data, and defines guidelines for updating those systems to a minimum standard.
- Build public-private partnerships managed by a central coordinating body to prioritize efforts to speed up the adoption and deployment of PQC in order to thwart risks associated with the threat of future decryption capabilities.
- Incentivize the adoption of PQC algorithms into commercial ICT products, transport protocols, and underlying ICT and internet infrastructure while encouraging the adoption of cryptographic agility across the private sector.

Incorporating AI

NSTAC acknowledges the substantive effort that resulted in the National Security Commission on Artificial Intelligence's report and recommends that the Administration give it due consideration, as it will lay the groundwork for further adoption and incorporation into broader ICT networks and applications. To that end:

- In building out Government networks, make use of

[65]National Security and Telecommunications Advisory Committee, "2017 NSTAC Report to the President on Emerging Technologies Strategic Vision," July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf

AI-driven orchestration and autonomous deployment technologies to incorporate the process of trust attestation in a shared-information model with ICT. This shared awareness of actionable operational and performance data will further enhance network security and reliability.

- Collaborate with industry to build out national AI/ML models for network optimization and anomaly detection in a way that is ubiquitous, extensible, and trustworthy.

Utilizing Testbeds to Enable Mastery of Quantum and AI Technologies

Testbeds: Quantum-Based Technologies

The Executive Branch should:

- Contract with a federally funded research and development center to create and manage a quantum "sandbox" that could serve as a testbed for near-term Government quantum application development.
- Develop a post-quantum cryptography testbed focused on transition challenges from legacy systems and algorithms.
- Coordinate with departments and agencies to incorporate best practices learned from testbed activities to drive awareness around quantum computing benefits and quantum security capabilities.

Government and industry should:

- Actively leverage and make more widely available quantum computing capabilities to solve complex problems, optimize network evolution and densification, and address resiliency and security challenges.
- Research approaches and technologies to mitigate the quantum computing threat to secure data at rest and in transit.

Testbeds: AI

Information sharing in the next evolution of network technologies and capabilities will be built upon machine-to-machine communication and supported by AI. To this end, the U.S. Government should:

- Encourage use of AI and ML to improve the effectiveness of network management and orchestration, as ML-based AI models are critical to bolstering the resiliency of the Nation's mission-critical communications networks going forward.
- Invest in building data sets to help train and test AI models to identify adversarial or anomalous behavior in networks based on operational data and automatically apply appropriate countermeasures for effective network defense or management.
- Fund and participate in testbeds for these technologies to extend the understanding of the advantages of AI/ML beyond the data science and AI communities into federal departments and agencies.

Conclusion

The seventh edition of the National Intelligence Council's Global Trends report outlines five future scenarios, three of which have direct relevance to this report: Renaissance of Democracies, Competitive Coexistence, and Separate Silos. Actions taken now will position the Nation to best lead the technology achievements outlined in the Renaissance scenario, to retain its competitiveness in the Coexistence scenario, and create a resilient, self-sufficient economy should the Separate Silos scenario come to fruition. While the report outlines some of the challenges the Nation faces, it highlights the evolution of the ICT ecosystem toward a highly resilient environment of federated, hyperconnected, distributed networks built on and managed by software.

With the advent of 5G and other network advances, the Nation now stands at a point where not only can the ICT providers create meshed and highly resilient operating environments, but enterprises (both Government and commercial) can avail themselves of these capabilities as well. It is NSTAC's contention that the resiliency benefits of new technologies and innovations referenced in this report position

the Nation's economy to not only derive cost and operational efficiencies, but to create an environment for U.S. innovation and leadership in the global economy. By adopting and mastering key technologies, NSTAC believes the Nation will be in a better position to support its national security, economic security, and emergency preparedness goals.

[66]Office of the Director of National Intelligence, "Global Trends 2040," 2021, https://www.dni.gov/index.php/global-trends-home

Appendix A. Subcommittee Membership

Mr. Angel Ruiz, MediaKind, Inc., Subcommittee Chair
Mr. Jeffrey Storey, Lumen Technologies, Inc., Subcommittee Chair
Mr. Jason Boswell, Ericsson, Inc., and Working Group Co-Lead
Ms. Kathryn Condello, Lumen Technologies, Inc., and Working Group Co-Lead

Mr. Christopher Anderson ..... Lumen Technologies, Inc.
Mr. Christopher Boyer ..... AT&T, Inc.
Mr. Billy Brown, Jr. ..... Cybersecurity and Infrastructure Security Agency
Mr. Jamie Brown ..... Tenable, Inc.
Mr. John Campbell ..... Iridium Communications, Inc.
Ms. Cheryl Davis ..... Oracle Corp.
Mr. Andrew Dugan ..... Lumen Technologies, Inc.
Mr. Paul Eisler ..... U.S. Telecom Association
Mr. Drew Epperson ..... Palo Alto Networks, Inc.
Mr. Jon Goding ..... Raytheon Technologies Corp.
Mr. Ani Karmarkar ..... Lockheed Martin Corp.
Mr. Kent Landfield ..... McAfee, LLC
Mr. Robert Mayer ..... U.S. Telecom Association
Mr. Sean Morgan ..... Palo Alto Networks, Inc.
Mr. Richard Mosley ..... AT&T, Inc.
Mr. Thomas Patterson ..... Unisys Corp.
Mr. Brian Peretti ..... Cybersecurity and Infrastructure Security Agency
Mr. John Peterson ..... Neustar, Inc.
Mr. Scott Poretsky ..... Ericsson, Inc.
Mr. Travis Russell ..... Oracle Corp.
Mr. Brett Scarborough ..... Raytheon Technologies Corp.
Mr. Chelsea Smethurst ..... Microsoft Corp.
Mr. Robert Spiger ..... Microsoft Corp.
Mr. Milan Vlajnic ..... Communication Technologies, Inc.
Mr. Peter White ..... AT&T, Inc.

Briefers: Subject Matter Experts

Mr. Scott Aaronson ..... Edison Electric Institute
Mr. Nipun Agarwal ..... Oracle Corp.
Mr. Adam Candeub ..... National Telecommunications and Information Administration
Mr. Roy Chua ..... AvidThink, LLC
Dr. Charles Clancy ..... MITRE Corp.
Mr. Lewis Curtis ..... Microsoft Corp.
Mr. Matthew Desch ..... Iridium Communications, Inc.
Mr. Andrew Dugan ..... Lumen Technologies, Inc.

Mr. Erik Ekudden ..... Ericsson, Inc.

Mr. Andre Feutsch ..... AT&T, Inc.

Mr. Steve Grobman ..... McAfee, LLC

Mr. Jay Heiser ..... Gartner, Inc.

Mr. Rob High ..... IBM Corp.

Dr. Mark Johnson ..... Oracle Corp.

Mr. Clete Johnson ..... Center for Strategic and International Studies

Ms. Lydia Leong ..... Gartner, Inc.

Mr. Mark Montgomery ..... Cyberspace Solarium Commission

Mr. Robert Morgus ..... Cyberspace Solarium Commission

Mr. Robert Olson ..... Palo Alto Networks, Inc.

Mr. Chris Pearson ..... 5G Americas

Ms. Allison Schwartz ..... D-Wave Systems, Inc

Dr. Louise Sengupta ..... Northrop Grumman Corp.

Mr. Kent Shuart ..... Verizon Communications, Inc.

Dr. Malik Tatipamula ..... Ericsson, Inc.

Dr. Michael Vermeer ..... RAND Corp.

Mr. Brad Whittington ..... Raytheon Technologies Corp.

Subcommittee Management

Ms. Sandra Benevides ..... President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO))

Ms. DeShelle Cleghorn ..... Alternate NSTAC DFO

Mr. Robert Greene ..... NSTAC Program Support

Ms. Sheila Becherer ..... Booz Allen Hamilton, Inc.

Ms. Emily Berg ..... Booz Allen Hamilton, Inc.

Mr. Philip Grant ..... Booz Allen Hamilton, Inc.

Mr. Ryan Garnowski ..... Insight Technology Solutions, LLC

Appendix B. Acronyms

4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
AAS	Advanced Antenna Systems
AI	Artificial Intelligence
AI/ML	Artificial Intelligence and Machine Learning
API	Application Programming Interface
BGP	Border Gateway Protocol
CDN	Content Delivery Network
CHIPS	Creating Helpful Incentives to Produce Semiconductors
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus
CR	Communications Resiliency
CSP	Cloud Service Provider
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DevOps	Development Operations
DFO	Designated Federal Officer
DHS	Department of Homeland Security
DL	Deep Learning
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoS	Denial-of-Service
DSR	Digital Silk Road
DSS	Dynamic Spectrum Sharing
EMP	Electromagnetic Pulse
EO	Executive Order
EOP	Executive Office of the President
FirstNet	First Responder Network Authority
GMD	Geomagnetic Disturbance
GPS	Global Positioning System
HEMP	High-Altitude Electromagnetic Pulse
HEO	Highly Elliptical Orbit

IaaS ..... Infrastructure-as-a-Service
ICT ..... Information and Communications Technology
IEEE ..... Institute of Electrical and Electronics Engineers
IETF ..... Internet Engineering Task Force
IoT ..... Internet of Things
IP ..... Internet Protocol
ISP ..... Internet Service Provider
IT ..... Information Technology
ITU ..... International Telecommunication Union
ITU-T ..... International Telecommunications Union Telecommunication Standardization Sector
IXP ..... Internet Exchange Point
KQI ..... Key Quality Indicators
LEO ..... Low Earth Orbit
LMR ..... Land Mobile Radio
LTE ..... Long-Term Evolution
LTO ..... Long-Term Outage
ML ..... Machine Learning
MSDR ..... Microsoft Services Disaster Response
MU-MIMO ..... Multi-User, Multiple-Input, Multiple-Output
NFV ..... Network Function Virtualization
NIST ..... National Institute of Standards and Technology
NLP ..... Natural Language Processing
NPSBN ..... National Public Safety Broadband Network
NRMC ..... National Risk Management Center
NSC ..... National Security Council
NS/EP ..... National Security and Emergency Preparedness
NSF ..... National Science Foundation
NSIC ..... National Supply Chain Intelligence Center
NSTAC ..... National Security Telecommunications Advisory Committee
NTIA ..... National Telecommunications and Information Administration
NTN ..... Non-Terrestrial Networks
ODNI ..... Office of the Director of National Intelligence
PNT ..... Positioning, Navigation, and Timing
PQC ..... Post-Quantum Cryptography
QC ..... Quantum Computing
QIS ..... Quantum Information Science

QKD ..... Quantum Key Distribution
QoS ..... Quality of Service
R&D ..... Research and Development
RAN ..... Radio Access Network
RBVM ..... Risk-Based Vulnerability Management
RF ..... Radio Frequency
RSA ..... Rivest-Shamir-Adleman
SaaS ..... Software-as-a-Service
SBA ..... Service-Based Architecture
SDN ..... Software-Defined Networking
SDO ..... Standards Development Organization
SME ..... Subject Matter Expert
SWaP ..... Size, Weight, and Power
UL ..... Underwriter Laboratories
UTM ..... Unified Threat Management
VoIP ..... Voice Over Internet Protocol
WAN ..... Wide Area Networking
ZTA ..... Zero-Trust Architecture

Appendix C. Definitions

Adaptive Networking: A new approach that expands on autonomous networking concepts to transform the static network into a dynamic, programmable environment driven by analytics and intelligence. (Cinea, https://www.ciena.com/insights/what-is/What-Is-the-Adaptive-Network.html#:~:text=The%20Adaptive%20Network%20is%20a%20new%20approach%20that,Public%20Switched%20Telephone%20Network%2C%20networks%20have%20continually%20evolved)

Advanced Antenna System: A combination of a radio antenna array and advanced software and hardware features. (Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/advanced-antenna-systems-for-5g-networks#:~:text=An%20advanced%20antenna%20system%20%28AAS%29%20is%20a%20combination,to%20support%20the%20execution%20of%20the%20AAS%20features)

Anomaly: An abnormal or outlying representation or behavior of or within a data set. (NIST, https://www.itl.nist.gov/div898/handbook/prc/section1/prc16.htm)

Application Programming Interface: A set of definitions and protocols for building and integrating application software. (Redhat, https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces)

Artificial Intelligence: The ability of a computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. (Loyola Marymount University, https://cs.lmu.edu/~ray/notes/introai/)

Border Gateway Protocol: A protocol that provides administrators with the ability to manage the routing of network traffic between tenants' virtual machine networks and their remote sites. (Microsoft, https://docs.microsoft.com/en-us/windows-server/remote/remote-access/bgp/border-gateway-protocol-bgp)

Broadband: High-speed internet access that is always on and faster than traditional dial-up access. (Federal Communications Commission [FCC], https://www.fcc.gov/general/types-broadband-connections#:~:text=The%20term%20broadband%20commonly%20refers%20to%20high-speed%20Internet,transmission%20technologies%20such%20as:%20Digital%20Subscriber%20Line%20

Cloud Computing: The delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet. (Microsoft Azure, https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/)

Commercial off-the-Shelf: Software and hardware that already exist and are available from commercial sources. (NIST SP 800-161 under Commercial off-the-shelf NIST SP 800-64 Rev. 2)

Communications Security, Reliability, and Interoperability Council: A body within the Federal Communications Commission responsible for providing recommendations regarding ways the government can strive for security, reliability, and interoperability of communications systems. (FCC, https://www.fcc.gov/file/12251/download)

Content Delivery Networks: A series of servers that are geographically dispersed to enable faster web performance by locating copies of web content closer to users or facilitating delivery of dynamic content. (IBM, https://www.ibm.com/cloud/learn/content-delivery-networks)

Critical Infrastructure: Sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. (CISA, https://www.cisa.gov/critical-infrastructure-sectors)

Connectivity: Capacity for the interconnection of platforms, systems, and applications. (PCMag, https://www.pcmag.com/encyclopedia/term/connectivity)

Counterfeit: An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. (NIST, NIST SP 800-161 18 U.S.C.)

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks. (Cisco, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of%20protecting%20systems,%20networks,,money%20from%20users;%20or%20interrupting%20normal%20business%20processes.)

Data Center: A physical facility that organizations use to house their critical applications and data. (Cisco, https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html#:~:text=At%20its%20simplest,%20a%20data%20center%20is%20a,enable%20the%20delivery%20of%20shared%20applications%20and%20data.)

Data Plane: An element of software that processes data and requests, passing them thereafter to their destination. (Microsoft, https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/control-plane-and-data-plane)

Deep Learning: A subset of machine learning in which multi-layered neural networks—modeled to work like the human brain—"learn" from large amounts of data. (IBM, https://www.ibm.com/cloud/learn/deep-learning)

Development Operations: The union of people, process, and technology, which strives to provide continuous value to information technology users. (Microsoft, https://azure.microsoft.com/en-us/overview/what-is-devops/)

Denial-of-Service: An action meant to shut down a machine or network, making it inaccessible to its intended users. (Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial-of-Service%20(DoS)%20attack%20is%20an%20attack%20meant,or%20sending%20it%20information%20that%20triggers%20a%20crash.)

Digital Silk Road: A Chinese program launched in 2015 as a component of Beijing's vast vision for global connectivity, the Belt and Road Initiative, which aims to improve digital connectivity in participating countries, with China as the main driver of the process. (The Diplomat, https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/)

Dynamic Spectrum Sharing: A process that allows an existing LTE carrier to operate 5G New Radio and LTE simultaneously – with a simple software upgrade. (Ericsson, https://www.ericsson.com/en/news/2019/9/ericsson-spectrum-sharing)

Edge Computing: A distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers. (IBM, https://www.ibm.com/cloud/what-is-edge-computing)

Emerging Technologies: Technologies that are currently developing and are expected to impact society in some significant way over the next 5 to 10 years. (Independence University, https://www.independence.edu/blog/what-is-emerging-technology)

Enterprise: An organization that coordinates the operation of one or more processing sites. (NIST SP 800-82 Rev. 2 under Enterprise ANSI/ISA-88.01-1995)

Fabrication: The process of manufacturing the microelectronic device in a foundry. (Science Direct, https://www.sciencedirect.com/topics/engineering/microelectronics-fabrication)

False Positive: An error in some evaluation process in which a condition tested for is mistakenly found to have been detected. (North Dakota State University, https://www.ndsu.edu/fileadmin/forward/climate_workshops/20101215_Worksheet_1.pdf)

Fifth Generation: The fifth installment of advanced wireless technology, bringing about increased bandwidth and capacity for advancements within the Internet of Things. (Qualcomm, https://www.qualcomm.com/5g/what-is-5g)

Fiber: Shorthand for "Fiber Optics," which is technology used to transmit information as pulses of light through strands of fiber made of glass or plastic over long distances. (Verizon, https://www.verizon.com/info/definitions/fiber-optics/)

Firewall: An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open. (NIST SP 800-82 Rev. 2 under Firewall ISA-62443-1-1)

Fourth Generation: The fourth installment of advanced wireless technology, best recognized by its association with long-term evolution broadband. (Academia, https://www.academia.edu/3099956/Generations_of_Wireless_Communication_From_0G_to_5G_Abhi)

Fourth Industrial Revolution: A phase of massive advancement in artificial intelligence, robotics, the Internet of Things, genetic engineering, quantum computing, and more. (Salesforce, https://www.salesforce.com/ap/blog/2020/03/apac-what-is-the-fourth-industrial-revolution-4IR.html)

Geomagnetic Disturbance: A major event in Earth's magnetosphere caused by a very efficient transfer of energy from solar wind into the space environment surrounding Earth. (NAES, https://www.naes.com/news/what-is-a-geomagnetic-disturbance-and-how-can-it-affect-the-power-grid/#:~:text=A%20geomagnetic%20disturbance%20 %28GMD%29%2C%20also%20known%20as%20a,solar%20wind%20into%20the%20space%20environment%20surrounding%20Earth)

Hardware: The physical components of an information system. (NIST SP 800-53 Rev. 4 under Hardware Committee on National Security Systems Instruction [CNSSI] 4009)

Hyperscalers: Large companies that manage scalable cloud computing systems in which a very large number of servers are networked together. (IONOS, https://www.ionos.com/digitalguide/server/know-how/what-is-hyperscale/)

Identity Centric: A robust security framework to ensure a specific, authorized user is accessing a network. (The Advanced Technology Academic Research Center, https://atarc.org/event/identity-centric-security/)

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (FIPS 200 under Information Technology 40 U.S.C., Sec. 1401)

Intelligence Community: Intelligence Community and elements of the Intelligence Community refers to the: (1) Office of the Director of National Intelligence; (2) Central Intelligence Agency; (3) National Security Agency; (4) Defense Intelligence Agency; (5) National Geospatial-Intelligence Agency; (6) National Reconnaissance Office; (7) other offices within DoD for the collection of specialized national foreign intelligence through reconnaissance programs; (8) intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps; (9) intelligence elements of the Federal Bureau of Investigation; (10) Office of National Security Intelligence of the Drug Enforcement Administration; (11) Office of Intelligence and Counterintelligence of the Department of Energy; (12) Bureau of Intelligence and Research of the Department of State; (13) Office of Intelligence and Analysis of the Department of the Treasury; (14) Office of Intelligence and Analysis of the Department of Homeland Security; (15) intelligence and counterintelligence elements of the U.S. Coast Guard; and (16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community. (CNSSI 4009-2015 EO 12333 (As amended by EOs 13284 (2003), 13355 (2004) and 13470 (2008))

International Telecommunication Union: The specialized United Nations agency for information and communication technologies. (ITU, https://www.itu.int/en/about/Pages/default.aspx)

Internet Exchange Points: A physical and usually neutral location where different IP networks meet to exchange local traffic via a switch. (Internet Society, https://www.internetsociety.org/issues/ixps/#:~:text=An%20 Internet%20Exchange%20Point%20(IXP)%20is%20a%20physical,of%20IXPs%20IXPs%20fall%20roughly%20 into%20five%20categories)

Internet of Things: A vast network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. (Oracle, https://www.oracle.com/internet-of-things/what-is-iot/)

Internet Protocol: Standard protocol for transmission of data from source to destinations in packet switched communications networks and interconnected systems of such networks. (CNSS, CNSSI 4009-2015)

Internet Service Providers: A company that provides internet connections and services to individuals and organizations. (Britannica, https://www.britannica.com/technology/Internet-service-provider)

Interconnectivity: The state of mutually connected technology. (Regulation Body of Knowledge, http://regulationbodyofknowledge.org/faq/telecommunication-regulation-interconnection/what-is-interconnection-and-why-is-it-important/#:~:text=Interconnection,%20which%20is%20the%20linking%20of%20 telecommunications%20networks,be%20able%20to%20communicate%20with%20all%20other%20customers)

Internet Bifurcation: The act of one entity, typically a nation-state, segmenting or portioning their internet access from the rest of the World Wide Web. (Science Direct, https://www.sciencedirect.com/science/article/abs/pii/S0096300318309731)

Interoperability: Ability of technologies to function in conjunction with one another. (Emergency Communication Networks, https://dps.mn.gov/divisions/ecn/programs/interoperability/Pages/default.aspx)

L-Band: The radio band containing frequencies from 1 to 2 GHz. (IEEE, https://www.tau.ac.il/~tsirel/dump/Static/knowino.org/wiki/IEEE_frequency_bands.html)

Latency: The delay before a transfer of data begins following an instruction for its transfer. (Independents Fiber Network, https://www.ifnetwork.biz/resources/blog/how-fiber-optic-networks-can-improve-speed-and-reliability-your-connectivity)

Long-Term Evolution: A standard of wireless broadband communication for mobile devices and cellular networks where the advantages of increased capacity are utilized. (Qualcomm, https://www.qualcomm.com/media/documents/files/download-the-evolution-of-mobile-technologies-1g-to-2g-to-3g-to-4g-lte-qualcomm.pdf)

Low-Latency: A rapid transmission of information across a network or between devices, with minimal timing between when a command is issued and when it is received. (Food and Drug Administration, https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-guides/glossary-computer-system-software-development-terminology-895)

Machine Learning: A branch of artificial intelligence focused on building applications that learn from data and improve their accuracy over time without being programmed to do so. (IBM, https://www.ibm.com/cloud/learn/machine-learning)

Malware: Software that is intended to damage or disable computers and computer systems. (McAfee, https://www.mcafee.com/en-us/antivirus/malware.html)

Management and Network Orchestration: The process of automating interactions across multiple types of devices, domains, and other related systems within a network. (Appview, https://www.appviewx.com/education-center/what-is-network-orchestration/)

National Security and Emergency Preparedness: A set of policy objectives calling for capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency. (https://larouchepub.com/eiw/public/1990/eirv17n45-19901123/eirv17n45-19901123_025-femas_blueprint_for_action_nsdd.pdf)

Natural Language Processing: A branch of computer science—and more specifically, the branch of artificial intelligence or AI—concerned with giving computers the ability to understand text and spoken words in much the same way human beings can. (IBM, https://www.ibm.com/cloud/learn/natural-language-processing)

Networks: A system of interconnected devices. (Britannica, https://www.britannica.com/technology/computer-network)

Network Latency: The time it takes for data to traverse a network and arrive at its destination. (Cisco, https://learningnetwork.cisco.com/s/question/0D53i00000Kt7e4/rtt-vs-delay-vs-latency)

Network Slicing: A method of creating unique logical and virtualized networks over a multi-domain infrastructure. (Researchgate, https://www.researchgate.net/publication/224146305_Virtualized_network_infrastructure_using_OpenFlow)

Network Virtualization: Abstracting – or virtualizing – network resources traditionally delivered in hardware to software. (VMware, https://www.vmware.com/topics/glossary/content/network-virtualization#:~:text=VMware%20NSX%20Data%20Center%20is%20a%20network%20virtualization,routing%20that%20are%20defined%20and%20consumed%20in%20software.)

Operating System: Software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals. (Arizona State University, https://courses.cpe.asu.edu/browse/mcs/courses/cpe-cidse-103)

Operational Technology: The use of hardware and software to monitor and control physical processes, devices, and infrastructure. (Forcepoint, https://www.forcepoint.com/cyber-edu/ot-operational-technology-security)

Packaging: The process of producing enclosures for one or more electronic chips using a substrate. (Smithsonian Institution, http://smithsonianchips.si.edu/chiptalk/icevocab.htm)

Post-Quantum Cryptography: Cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. (NIST, https://csrc.nist.gov/projects/post-quantum-cryptography)

Protocol: A set of rules governing the exchange or transmission of data between devices. (Computer Science Principles, https://curriculum.code.org/csp-19/unit1/3/#:~:text=Protocol%20-%20A%20set%20of%20rules%20governing%20the,governs%20how%20devices%20should%20transmit%20and%20interpret%20data.)

Quality of Service: A set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. (Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos)

Quantum Computing: A computer architecture based on quantum mechanics. (Microsoft, https://docs.microsoft.com/en-us/azure/quantum/overview-understanding-quantum-computing)

Quantum Key Distribution: A process that utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology (National Security Agency, https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/)

Radio-Access Network: A central element of a telecommunications system that connects devices to other parts of a network through radio technology. (Verizon, https://www.verizon.com/about/our-company/5g/5g-radio-access-networks)

Risk-Based Vulnerability Management: A process that reduces vulnerabilities across an attack surface by prioritizing remediation based on the risks they pose to an organization (Tenable, https://www.tenable.com/risk-based-vulnerability-management#:~:text=Risk-based%20vulnerability%20management%20%28RBVM%29%20is%20a%20process%20that,risk-based%20vulnerability%20management%20goes%20beyond%20just%20discovering%20vulnerabilities)

Satellite: An artificial body placed in orbit around the earth or moon in order to send and receive information, such as for communication. (NASA, https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-a-satellite-58.html)

Silicon: A nonmetal with semiconducting properties, used in making electronic circuits. (Encyclopedia, https://www.encyclopedia.com/science-and-technology/chemistry/compounds-and-elements/silicon)

Sixth Generation: An emerging, sixth generation of wireless communications technologies over cellular networks. (Researchgate, https://www.researchgate.net/publication/341017368_Sixth_Generation_6G_Wireless_Networks_Vision_Research_Activities_Challenges_and_Potential_Solutions)

Software Applications: An application is any program, or group of programs, that is designed for the end user. Applications software (also called end-user programs) include such things as database programs, word processors, web browsers, and spreadsheets. (Webopedia, https://www.webopedia.com/definitions/application-software/#:~:text=App%20is%20used%20to%20describe%20a%20type%20of,article%20was%20updated%20April%202021%20by%20Jenna%20Phipps)

Software Infrastructure: Infrastructure software is a type of enterprise software or program specifically designed to help business organizations perform basic tasks such as workforce support, business transactions, and internal services and processes. The most common examples of infrastructure software are database programs, email and other communication software, and security applications. (Techopedia, https://www.techopedia.com/definition/26477/infrastructure-software)

Software-as-a-Service: A system that allows users to connect to and use cloud-based apps over the internet, such as email and calendaring tools. (General Services Administration, https://cic.gsa.gov/solutions/saas)

Software-Defined Networking: An architecture that gives networks more programmability and flexibility by separating their control plane from a data plane. (Avi Networks, https://avinetworks.com/glossary/software-defined-application-services/)

System on Chip: A circuit embedded on a small coin-sized chip and integrated with a microcontroller or microprocessor. (Washington, https://courses.cs.washington.edu/courses/cse466/15au/pdfs/lectures/02-Microprocessors-Microcontrollers.pdf)

Telecommunications: Information exchange and transmission by way of various types of technologies over wire, radio, optical, or other electromagnetic systems. (Microsoft Academic, https://academic.microsoft.com/topic/76155785)

Transport Layer Security: An encryption protocol intended to keep data secure when being transferred over a network. (Norton, https://us.norton.com/internetsecurity-privacy-what-is-encryption.html)

Trusted Internet Connection (TIC): A federal cybersecurity initiative intended to enhance network and boundary security across the Federal Government. The Government has developed use cases for the recent TIC 3.0 guidance to focus on items like zero-trust and other emerging capabilities across Government and industry.(Cisco, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/NetworkTIC_wp.pdf)

Unified Threat Management: A system that provides multiple security features and services in a single device or service on the network, protecting users from security threats in a simplified way (Juniper, https://www.juniper.net/us/en/products-services/what-is/utm/)

Unmanned Aerial Vehicle: An aircraft piloted by remote control or onboard computers. (Percepto, https://percepto.co/what-are-the-differences-between-uav-uas-and-autonomous-drones/)

Virtualization: The simulation of the software and/or hardware upon which other software runs. (NIST, NIST SP 800-125)

Voice over Internet Protocols: A technology that allows the user to make voice calls using a broadband internet connection instead of a regular phone. (FCC, https://www.fcc.gov/general/voice-over-internet-protocol-voip#:~:text=Voice%20over%20Internet%20Protocol%20%28VoIP%29%2C%20is%20a%20technology,instead%20of%20a%20regular%20%28or%20analog%29%20phone%20line)

Wide-Area Networking: A collection of local-area or other networks that communicate with one another. (Cisco, https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html#:~:text=In%20its%20simplest%20form%2C%20a%20wide-area%20network%20%28WAN%29,networks%2C%20with%20the%20Internet%20the%20world%27s%20largest%20WAN.)

Wireless Local Area Network: A local area network that does not rely on wired Ethernet connections. It can be either an extension to a current wired network or an alternative to it. (Indiana University, www.kb.iu.edu/d/aick)

Zero-Trust Architecture: An architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized. (NIST, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture)

Appendix D. Bibliography

Aaronson, Scott, Edison Electric Institute, "Communications Resiliency Briefing" (Briefing to the NSTAC Communications Resiliency [CR] Subcommittee, Arlington, VA, October 22, 2020)

ABI Research, "54 Technology Trends to Watch in 2020," 2020, https://www.abiresearch.com/pages/54-trends/

Agarwal, Nipun, Oracle, "Machine Learning Opportunities and Direction" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 22, 2020)

Antichi, Gianni, Böttger, Timm, Castro, Ignacio, Fernandes, Eder L., Lallo, Roberto di, Uhlig, Steve, "The Elusive Internet Flattening: 10 Years of IXP Growth," November 7, 2021, https://www.researchgate.net/publication/328528921_The_Elusive_Internet_Flattening_10_Years_of_IXP_Growth

AT&T, "Cybersecurity Insights Report, Tenth Edition: 5G and the Journey to the Edge," 2021, https://cdn-cybersecurity.att.com/docs/whitepapers/cybersecurity-insights-report-tenth-edition.pdf

Australian Government Department of Home Affairs, Critical Infrastructure Center, "Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Document," November 2020, https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf

Baran, Paul, RAND, "On Distributed Communications," http://www.cybertelecom.org/notes/baran.htm

Broadband Deployment Advisory Committee to the Federal Communications Commission, "Report and Recommendations: COVID-19 Response," October 29, 2020, https://www.fcc.gov/sites/default/files/bdac-disaster-response-recovery-approved-rec-10292020.pdf

Brock, Alexander, MIT Technology Review, "5G and the Enterprise Opportunity," October 7, 2020, https://www.technologyreview.com/2020/10/07/1009178/5g-and-the-enterprise-opportunity/

Candeub, Adam, National Telecommunications and Information Administration, "NTIA's Vision for Secure Networks in 2030" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 10, 2019)

Center for Strategic & International Studies Working Group on Trust and Security in 5G Networks, "Criteria for Security and Trust in Telecommunications Networks and Services," May 2020, https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services#:~:text=Criteria%20for%20Security%20and%20Trust%20in%20Telecommunications%20Networks,to%20Increase%20Confidence%20in%20Choosing%20a%20Supplier.%20

Chua, Roy, AvidThink, "Communications Resilience in 2030" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 8, 2020)

Chuin-Wei Yap, Wall Street Journal, "State Support Helped Fuel Huawei's Global Rise," December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736

Clancy, Charles, MITRE, "Internet Futures: Challenges and Opportunities" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 3, 2020)

Cloud Smart, "From Cloud First to Cloud Smart," 2021, https://cloud.cio.gov/strategy/

Collinson, Andrew and Barraclough, Chris, "Telco 2030: New Purpose, Strategy and Business Models for the Coordination Age," December 2019, https://stlpartners.com/research/telco-2030-new-purpose-strategy-and-business-models-for-the-coordination-age/

Council to Secure the Digital Economy, International Botnet and IoT Security Guide 2021, https://securingdigitaleconomy.org/projects/international-anti-botnet-guide/

Craft, James et al, "COVID-19 Compels Better NSEP Planning," July 2020, https://www.afcea.org/signal/resources/linkreq.cfm?id=270

Cross Mission Ground and Communications Enterprise Directorate, "Request for Information (RFI) for 5G for Space Data Transport (SDT)," https://beta.sam.gov/opp/8edcadbb56764ca1a53f7cf6322c76d5/view?keywords=AR11&sort=-modifiedDate&index=&is_active=true&page=1

Curtis, Lewis, Microsfot, "Microsoft Services Disaster Response" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 5, 2020)

Cybersecurity and Infrastructure Security Agency, "Electromagnetic Pulse and Geomagnetic Disturbance," https://www.cisa.gov/emp-gmd

Cybersecurity and Infrastructure Security Agency, "Electromagnetic Pulse Program Report," https://www.cisa.gov/publication/emp-program-status-report

Cybersecurity and Infrastructure Security Agency, "Priority Telecommunications Services," April 9, 2020, https://www.cisa.gov/pts

Cybersecurity and Infrastructure Security Agency, "Telecommunications Service Priority," January 23, 2020, https://www.cisa.gov/telecommunications-service-priority-tsp

Cyberspace Solarium Commission, "Transition Book for the Incoming Biden Administration," January 2021, https://www.solarium.gov/public-communications/transition-book

Cyphers, Bennet, Electronic Frontier Foundation, "The Case for Fiber to the Home, Today: Why Fiber is a Superior Medium for 21st Century Broadband," October 16, 2019, https://www.eff.org/wp/case-fiber-home-today-why-fiber-superior-medium-21st-century-broadband

Deloitte Insights, "Tech Trends 2021," 2020, https://www2.deloitte.com/us/en/insights/focus/tech-rends.html

Department of Energy, "The Smart Grid," https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Department of Homeland Security, "DHS Publishes Free Resources to Protect Critical Infrastructure from GPS Spoofing" February 26, 2021, https://www.dhs.gov/science-and-technology/news/2021/02/26/news-release-dhs-publishes-free-resources-protect-critical-infrastructure-from-gps-spoofing

Department of Homeland Security, "Electromagnetic Pulse Program Status Report," August 17, 2020, https://www.cisa.gov/publication/emp-program-status-report

Department of Homeland Security, "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," December 2020, https://www.hsdl.org/?view&did=848704

Department of Homeland Security, "Positioning, Navigation, and Timing (PNT) Program," 2020, https://www.dhs.gov/science-and-technology/pnt-program

Department of Homeland Security Office of Strategy, Policy, and Plans, "DHS Strategic Action Plan to Counter the Threat Posed by the People's Republic of China," 2020, https://www.dhs.gov/sites/default/files/publications/21_0112_plcy_dhs-china-sap.pdf

Department of Homeland Security Science and Technology Directorate, "Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework," August 2020, https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework

Desch, Matthew, Iridium Communications, "NSTAC Communications Resiliency Briefing" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 15, 2020)

Doubleday, Justin, Inside Cybersecurity, "Artificial Intelligence Commission recommends major funding shifts to fuel Pentagon AI advances," February 19, 2020, https://insidecybersecurity.com/daily-news/artificial-intelligence-commission-recommends-major-funding-shifts-fuel-pentagon-ai

Dugan, Andrew, Lumen Technologies, "The Future of Networking" (Briefing to the NSTAC CR Subcommittee. Arlington, VA, December 1 and 10, 2020)

European Union Agency for Cybersecurity, "Network and Information Security Directive," July 2016, https://www.enisa.europa.eu/topics/nis-directive

European Telecommunications Network Operators' Association, "ETNO Position Paper on the New IP Proposal," November 2020, https://www.etno.eu/library/positionpapers/417-new-ip.html#:~:text=ETNO%20position%20paper%20on%20the%20New%20IP%20proposal.,the%20European%20telecommunications%20sector%20on%20this%20important%20issue

Executive Office of the President, "Executive Order 13865: Coordinating National Resilience to Electromagnetic Pulses," March 26, 2019, https://www.federalregister.gov/documents/2019/03/29/2019-06325/coordinating-national-resilience-to-electromagnetic-pulses

Executive Office of the President, "EO 13905: Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," February 18, 2020, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

Feutsch, Andre, AT&T, "AT&T: Connecting the Future" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, January 12, 2021)

FirstNet Authority, "First Responder Network Authority Roadmap," October 27, 2020, https://firstnet.gov/sites/default/files/Roadmap_2020_nocompress.pdf

Gallagher, Mike and King, Angus, "Cyberspace Solarium Commission," March 2020, https://www.fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf

GPS.gov, "LORAN-C Infrastructure and E-Loran", 2019, https://www.gps.gov/policy/legislation/loran-c/

Grobman, Steve, McAfee, "Artificial Intelligence and the Adversary" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 10, 2020)

Hanke, Steve, Yahoo! News, "China Rattles Its Rare-Earth-Minerals Saber, Again," February 25, 2021, https://news.yahoo.com/china-rattles-rare-earth-minerals-113020191.html

Heiser, Jay and Leong, Lydia, Gartner, "The Public Cloud is the Most Critical Part of Our Digital Infrastructure" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 15, 2020).

High, Robert, IBM, "IBM Perspectives on 5G and Edge Trends and Threats" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 17, 2020)

Homeland Security Advisory Council, "Final Report: Economic Security Subcommittee," November 2020, https://www.dhs.gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf

Hosenball, Mark, Reuters, "Biden Intelligence Pick to Call for Tough Scrutiny of China, Source Says," January 19, 2021, https://www.reuters.com/article/usa-biden-intelligence/biden-intelligence-pick-to-call-for-tough-scrutiny-of-china-source-says-idUSL1N2JP3BE

IETF, Liaison statement: Response to "LS on New IP, Shaping Future Network," March 30, 2020, https://datatracker.ietf.org/liaison/1677/

IBM, "What is Software Defined Networking (SDN)?" https://www.ibm.com/services/network/sdn-versus-traditional-networking

Johnson, Clete, Center for Strategic and International Studies, "China, the COVID-19 Pandemic, and the Future of Communications Security and Reliability" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 29, 2020)

Johnston, Hamish, "Quantum cryptography network spans 4600 km in China," January 7, 2021, https://physicsworld.com/a/quantum-cryptography-network-spans-4600-km-in-china/

Johnson, Mark, Oracle, "Opportunities and Risks with Natural Language Processing and Artificial Intelligence" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 27, 2020)

Langan-Riekhof, Maria and Hahs, Brian, Office of the Director of National Intelligence, "Global Trends" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 3, 2020)

Ley, Daniel, Schwartz, Allison, Condello, Alexander, D-Wave, "Practical Quantum Computing: Quantum and Hybrid Solutions for Communications Resiliency" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, January 5, 2021)

Maurer, Tim and Nelson, Arthur, "International Strategy to Better Protect the Financial System Against Cyber Threats," 2020, https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf

MIT Technology Review, "5G and the Enterprise Opportunity," October 7, 2020, https://www.technologyreview.com/2020/10/07/1009178/5g-and-the-enterprise-opportunity/

Mohammed, Abdul Jabbar, Hutchison, David, and Sterbenz, James, "Towards Quantifying Metrics for Resilient and Survivable Networks," https://resilinets.org/papers/Mohammad-Hutchison-Sterbenz-2006.pdf

Montgomery, Mark, and Morgus, Robert, Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 19, 2020)

National Defense University, "Severe Space Weather Threats: National Electrical Grid and Impacts to Critical Infrastructures – After Action Report," 2011

National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0" February 18, 2021, https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40

National Institute of Standards and Technology, "NIST's Quantum Logic Clock Returns to Top Performance" July 2019, https://www.nist.gov/news-events/news/2019/07/nists-quantum-logic-clock-returns-top-performance

National Institute of Standards and Technology, "Quantifying Operational Resilience Benefits of the Smart Grid," February 2021, https://www.nist.gov/publications/quantifying-operational-resilience-benefits-smart-grid

National Institute of Standards and Technology, "Zero-Trust Architecture," https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture#:~:text=In%20November%202019%2C%20the%20NCCoE%20and%20the%20Federal,in%20the%20federal%20government%20and%20the%20commercial%20sector

National Intelligence Council, "Global Trends 2030: Alternative Worlds," December 2012, https://www.dni.gov/files/documents/GlobalTrends_2030.pdf

National Quantum Coordination Office, "DOE Quantum Research Center Announces Quantum Computing Summer School," March 30, 2021, https://www.quantum.gov/doe-quantum-research-center-announces-quantum-computing-summer-school/

National Security Agency, "Embracing a Zero-Trust Security Model," February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

National Security and Telecommunications Advisory Council, "2008-2009 NSTAC Issue Review," 2009, https://www.cisa.gov/sites/default/files/publications/2008-2009%20NSTAC%20Issue%20Review.pdf

National Security and Telecommunications Advisory Committee, "2008 NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System" 2008, https://www.cisa.gov/sites/default/files/publications/NSTAC%20GPS%20Report_0.pdf

National Security and Telecommunications Advisory Committee, "2017 NSTAC Report to the President on Emerging Technologies Strategic Vision," July 14, 2017, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf

National Security and Telecommunications Advisory Committee, "2019 NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem," September 3, 2019, https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_2.pdf

National Security Commission on Artificial Intelligence, "Final Report," 2021, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2021/mar/cs2021_0042.pdf

National Security Council, "Communications Dependency on Electric Power Working Group Report: Long-Term Outage Study," 2009, https://www.hsdl.org/?view&did=13836

Office of the Director of National Intelligence, "Global Trends 2040," 2021, https://www.dni.gov/index.php/global-trends-home

Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China," 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

Olson, Ryan, Palo Alto Networks, "SolarWinds Software Supply Chain Attack" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, January 7, 2021)

Osipovich, Alexander, "High-Frequency Traders Push Closer to Light Speed With Cutting-Edge Cables," December 15, 2020, https://www.wsj.com/articles/high-frequency-traders-push-closer-to-light-speed-with-cutting-edge-cables-11608028200

Parkinson, Ed and Bratcher, Jeff, FirstNet, "FirstNet: Out Nation's Public Safety Network" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 3, 2020)

Pearson, Christopher, 5G Americas, "Mobile Wireless Trends" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 17, 2020)

Pressman, Aaron, Fortune, "The Great Chip Shortage of 2021: Why Carmakers and Computer makers Are Scrambling," February 15, 2021, https://fortune.com/2021/02/15/chip-shortage-2021-cars-computers-auto-industry-technology-covid-19/

Priddle, Alisa, Motortrend, "Ford Cuts F-150 Production Due to Semiconductor Chip Shortage," February 5, 2021, https://www.motortrend.com/news/semiconductor-chip-shortage-automotive-ford-f-150/

Pro-Vigil, "The State of Physical Security Entering 2021," 2020, https://pro-vigil.com/secure/security-survey-report/

Rebbeck, Tom and Sale, Stephen, "The pandemic has not led to many strategy changes for operators, but some aspects require and rethink," January 2021, https://www.analysysmason.com/contentassets/b9feca017b1f418592f8347866bb664c/analysys_mason_post_pandemic_landscape_jan2021_ren01_ren02_rdmz0_rdmm0_rdmb0_rdmd0_rdmv0_rdmy0_rdcs0_rdvs0.pdf

Renewing America's Advantages - Interim National Security Strategic Guidance, The White House, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

Resilient Navigation and Timing Foundation, "A Resilient National Timing Architecture," October 16, 2020, https://rntfnd.org/wp-content/uploads/Resilient-National-Timing-Architecture-16-Oct-2020.pdf

Rohner, Boyden, CISA, "Vulnerability Management Perspective on Continuity of Communications" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, January 7, 2021)

Semiconductor Industry Association, "CHIPS for America Act Would Strengthen U.S. Semiconductor Manufacturing, Innovation" June 10, 2020, https://www.semiconductors.org/chips-for-america-act-would-strengthen-u-s-semiconductor-manufacturing-innovation/

Sengupta, Louise, Northrop Grumman, "The Effect of the Digital Transformation on the Security of Microelectrics" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, November 17, 2020)

Shead, Sam, CNBC, "Carmakers Have been Hit Hard by a Global Chip Shortage — Here's Why," February 8, 2021, https://www.cnbc.com/2021/02/08/carmakers-have-been-hit-hard-by-a-global-chip-shortage-heres-why-.html

Shuart, Kent and Lee, Vincent, Verizon, "The View from 2030 on the Cyber Disruption Pandemic" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 15, 2020)

Susser, Jonathan, Advanced Energy, "The Evolving Electric Power Grid," February 27, 2020, https://www.advancedenergy.org/2020/02/27/the-evolving-electric-power-grid/

Tatipamula, Mallik and Ekudden, Erik, Ericsson, "Future Technology Trends and Ericsson's Outlook Towards 6G" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, December 10, 2020)

Tenable, "Tenable's 2020 Threat Landscape Retrospective," 2020, https://www.tenable.com/cyber-exposure/2020-threat-landscape-retrospective

United States Congress, "CHIPS for America Act", June 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3933/text

United States Congress, "Fiscal Year 2021 National Defense Authorization Act," January 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395/text

United States Congress, "National Timing and Resiliency Act of 2017", December 2017, https://www.congress.gov/bill/115th-congress/senate-bill/2220

University of Science and Technology of China, "world's first integrated quantum communication network," January 6, 2021, https://phys.org/news/2021-01-world-quantum-network.html

Van der Meulen, Rob, Gartner, "What Edge Computing Means for Infrastructure and Operations Leaders," October 3, 2018, https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/

Vermeer, Michael, RAND, "Managing the Risks to U.S. Communications Resiliency from Quantum" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 15, 2020)

Vermeer, Michael, RAND, "Securing Communications in the Quantum Computing Age," 2020, https://www.rand.org/pubs/research_reports/RR3102.html

Whittington, Brad, Raytheon Technologies, "Defense Industrial Base Observations on 5G and National Security" (Briefing to the NSTAC CR Subcommittee, Arlington, VA, October 20, 2020)

Winks, David, "Protecting U.S. Electric Grid Communications From Electromagnetic Pulse," May 2020, https://www.resilientsocieties.org/uploads/5/4/0/0/54008795/protecting_us_electric_grid_communications_from_emp.pdf

World Economic Forum, "The Global Risks Report 2021," 2021, http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

Yirka, Bob "Using drones to create local quantum networks," January 18, 2021, https://phys.org/news/2021-01-drones-local-quantum-networks.html