THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Emerging Technologies Strategic Vision

TBD

DRAFT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Government will face unprecedented growth and transformation in the technology ecosystem over the next decade. Multiple waves of innovation, involving both new and evolving technologies, will alter the fabric of the digital and physical environment, ultimately changing how we live and work. Greater interconnectivity and processing power, combined with new capabilities in analytics, cognition, and autonomy, will allow computers to make decisions across a range of domains. Developments in production and simulation will enable technology to proliferate beyond current conceptions of devices and integrate both physical and virtual environments. Methods of trust and verification will be distributed across the technology ecosystem and increase real-time visibility.

Recent and forthcoming innovations and changes have been and will continue to be interrelated, increasing the importance of understanding deployment timelines and dependencies among technologies. Specifically, some technology trends and developments help to advance, delay, or alter the arrival, evolution, or proliferation of others. For example, increases in interconnectivity and processing power enable more precise analytics, more powerful cognition, and greater autonomy. The production of nanoscale devices facilitates connectivity, and virtual environments may act as platforms that both use and generate data analytics and new trust methods. Similarly, technology involving analytics, including machine learning and artificial intelligence (AI), will permit new verification methods that may increase—or decrease—trust. However, where the deployment of high capacity and high quality wireless technology (e.g., 5G) is limited, the deployment of advanced virtual or augmented reality technologies will stall.

Within each trend of forthcoming innovation, such as interconnectivity and processing power, there are both near- and long-term developments to consider. While truly revolutionary change is not yet close enough to describe with certainty, the President's National Security Telecommunications Advisory Committee (NSTAC) found experts in broad agreement that certain dramatic advancements are foreseeable. Quantum computing will revolutionize information and communications technologies (ICT) in ways that push beyond our current conceptions, and the notion of a quantum computer capable of defeating widespread encryption systems is no longer that of speculation—only the precise timing and ownership are still in question. Biomorphic computing, nanotechnology, and advanced materials science are, like quantum, foreseeable developments that will disrupt entire disciplines.

How should the Government think about and prepare for this unprecedented growth and transformation in the technology ecosystem, both in the near and long term? What opportunities and risks should the Government assess to determine whether and how to invest in and deploy various emerging technologies? And how can the Government ensure that the impacts of these technology developments on the Government's national security and emergency preparedness (NS/EP) functions are both well understood and appropriately addressed?

The purpose of this NSTAC report is to provide guidance on these and related questions. Throughout its examination, the NSTAC consistently found 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, a consistent theme of this

report is that the Government must harvest the significant NS/EP benefits of forthcoming technology while also addressing new threats and vulnerabilities.

The NSTAC also considered the context in which it is delivering this report; the Government and private sector face a range of daunting technical and non-technical cybersecurity challenges. These challenges include a tense international environment, a high level of adversarial activity by both nation-state and non-state actors, and deficiencies in the development or deployment of security techniques and capabilities. In this environment, maintaining the status quo is inadequate and unacceptable. The Government must act with unprecedented speed and rigor to address cybersecurity challenges, making fiscal and regulatory commitments that enable upgrades in technology and utilizing security models that improve governance and operational efficiency. Ultimately, investments in national infrastructure must be paralleled or even exceeded by a commitment to securing cyber elements, and that commitment must be established amidst and reinforced by multiple waves of forthcoming innovation.

Technology Overview

The technologies discussed within this report are complex and interdependent and have varying degrees of predictability; however, there are several organizing and interrelated trends: interconnectivity and processing power; analytics, cognition, and autonomy; production and simulation; and trust and verification.

Interconnectivity and Processing Power

Over the last two decades, billions of people and things—including personal computers, mobile devices, wearable devices, home appliances, and sensors—have been connecting to networks and to each other. Each of those devices has been powered in accordance with Moore's Law,[1] as electronics have become less expensive, more compact, and better performing. Meanwhile, connections between an ever-increasing number of devices have been supported by improving wireless technologies (e.g., 4G), Internet Protocol (IP) version 6, and other developments that increase the speed, availability, and bandwidth of network connections.

This trend represents the next advancements in this continuing evolution, including software-defined networks (SDN) and network function virtualization (NFV), which will ultimately transform ICT architecture. These advancements began with the arrival of cloud computing, an enabling technology that disrupted the traditional enterprise network architecture by pooling computing resources used across multiple enterprises and creating "virtual machines." Going forward, networks will also transform from static physical infrastructures to virtual ones in which software residing on generic platforms replaces physical devices. At the same time, rapidly proliferating Internet of Things (IoT) sensors and control devices will leverage higher capacity and higher quality wireless technology as well as meshed networks to add ubiquitous connectivity and unimaginable amounts of data. In the long term, quantum computing and other advanced computing architectures will emerge and transcend Moore's Law.

[1] Moore's Law states that technology continually expands at an exponential and measurable rate or, more commonly, that computer power doubles every two years at the same cost. The Economist. "Technology Quarterly: After Moore's Law," March 12, 2016. Available at: http://www.economist.com/technology-quarterly/2016-03-12/after-moores-law.

This highly ubiquitous, dynamic, virtual, and data rich ICT architecture could greatly enhance the Government's ICT access and agility as well as its ability to respond to and recover from emergency situations. This architecture will also be more complex and less predictable, so the Government will need well-integrated, strategic plans to ensure resiliency. Considering how NS/EP functions are impacted by the new environment will become more difficult—but more important—since the new architecture will control not just critical information but also critical devices and infrastructures in the physical world. Moreover, there is a serious imperative for the Government to understand and prepare for the NS/EP implications of quantum computing.

Analytics, Cognition, and Autonomy

More devices, more data, increasingly pooled and shared data across environments, and better connectivity is just the beginning of the story. Connecting machines, screens, sensors, and people will also enable and improve machine learning and AI, powering advancements across a wide range of human activities. Indeed, AI is as significant for the next waves of innovation as the invention of electricity was for the 20th century. The next several years will see the advent of AI-driven software and autonomous machines capable of greatly augmenting human capability as well as performing tasks that were formerly reserved for humans. Great opportunity is inherent in these developments, along with the potential for significant risks.

This trend of analytics, cognition, and autonomy captures current, forthcoming, and speculative technologies and abilities to process, make sense of, and apply large amounts of information to resolve questions, discover and share insights, and act—both with and without humans. Near-term AI includes forms that are currently being commercialized and developments that will lead to advances in medical diagnosis, automated security, and language translation. In the long term, technologies that power autonomous vehicles will proliferate. Experts also expect that more mature forms of sentient or even sapient AI will emerge, although the exact range of capabilities and degree of intelligence or autonomy that will be embedded in this future AI is unclear.

Here again, the challenge for the Government is to realize the enormous NS/EP benefits of AI developments while mitigating the risks. However, beyond that, the Government will need to get ahead of the technology and consider appropriate norms for the ecosystem around AI and the behavior of autonomous machines. As with other technologies, but in particular in the case of AI, the Government should also consider international adoption and use, which may be progressing more rapidly than domestic use. In addition, the Government should consider how to prepare for the potentially disruptive social impacts of AI and autonomous machines as well as the need for employees with radically new job skills.

Production and Simulation

Society is amidst a major shift from an industrial age to an information age. We are shifting from analog to digital technology and from entirely physical to a mix of physical and virtual. Moreover, what is physically possible is shifting as advanced materials can increasingly be integrated into everyday objects and new, nanoscale devices. These shifts are manifesting in a range of ways, including how society views and shares information, how products or services can be customized for individual users, and what qualifies as an ICT device.

This trend captures forthcoming changes in the materials used for production; ways to simulate, analyze, and improve production; and platforms to experience and interact in both the real and simulated world. This trend will likely result in lower cost, more efficient, and more iterative technology development; greater potential for personalization, shared resources, and interactive learning; and more flexibility in environmental requirements. Technologies that fit within this trend, including ubiquitous screens, virtual and augmented reality, 3D and 4D printing, and active nanotechnology, will emerge and evolve over the near and long term. They will be advanced and enhanced by technologies described within other trends, including 5G and AI.

These technologies may substantially augment various NS/EP functions. For example, 3D printing could be used to meet the materials needs of first responders, and virtual and augmented reality could not only help prepare first responders and military personnel for deployment but also be used to direct resources (e.g., remote medical assistance) during a disaster. Alternatively, an adversary may disrupt or hijack the use of these technologies or independently use these technologies to operate with greater agility. As in the context of other trends, these technologies are generating new capabilities that will benefit the Government's NS/EP mission, but the Government must also be cognizant of and work to mitigate potential risks.

Trust and Verification

How we enable trusted communications and verify identities (regardless of the platform or activity) will become increasingly important as ubiquitous connectivity, intelligence, and virtual platforms are integrated into nearly every aspect of everyday life. As such, amidst broader ecosystem changes, many of which will result in new security benefits and risks, there are also forthcoming developments around technologies that focus on furthering trust and methods of verification. Specifically, there are new and evolving ways of ensuring the confidentiality, integrity, and availability of information and communication.

In the near term, technologies and risk management processes, including cybersecurity platforms and information sharing, will help to gain real-time visibility across a range of users and environments. This visibility, coupled with advances in big data, real-time analytics, and AI, will help to mitigate risks and evolve defensive tactics. In addition, there will be an increasing need to have trust across a distributed, ubiquitous, and integrated ICT architecture. As such, use of biometric information to verify identities, including through mobile and other devices, will proliferate. Technologies that are especially relevant for decentralized systems, including blockchain, will also increase in relevance, and over the long term, technologies that are responsive to new risks, including quantum-resistant encryption, will be deployed.

Consistent with the approach required in the above-described trends, the Government must recognize the NS/EP benefits of these technologies while also considering their limitations and the new threats that they may create, including loss or alteration of biometric data and dependence on blockchain technologies. Additionally, the Government should recognize the importance of not only using but also preparing to use advanced security technologies that are responsive to advanced threats. In particular, preparing to deploy quantum-resistant encryption will be critical to ensuring ongoing trust in the rapidly advancing technology ecosystem.

Recommendations

Based on our findings across technologies and trends, the NSTAC developed a set of recommendations, highlighting opportunities and areas of concern. While the recommendations are not listed in order of priority or importance, they are organized under three headings:

- "High-priority actions" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for near-term technology developments;

- "Strategic opportunities" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for long-term technology developments; and

- "Cross-technology imperatives" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for multiple near- and long-term technology developments.

High-Priority Actions:

- **Develop a Strategic Plan to Modernize ICT Network Architecture in Support of the Government's NS/EP Mission.**

    - The Government should leverage shared infrastructure and common services, including cloud computing and SDN/NFV, as well as a more integrated approach to incorporating innovative technologies across the Government.

    - The Government should develop a policy and plan, similar to that developed for cloud computing, for the efficient acquisition and implementation of SDN and NFV in Federal networks. In doing so, the Government should assess which networks should be slated for accelerated upgrade or replacement, and oversight should be established to ensure that critical upgrades and required changes are made with sufficient urgency.

    - The Government should evolve existing Federal and critical infrastructure protection guidance to incorporate SDN/NFV developments. In particular, in consultation with infrastructure operators, the Department of Homeland Security should: (1) review the effects of SDN/NFV on the existing critical infrastructure taxonomy; and (2) support NS/EP planners in identifying key virtual assets in critical infrastructure and leveraging SDN/NFV for response and recovery efforts.

    - The Government should streamline the regulatory approval process for 5G technology to facilitate its rapid deployment and enable other technology developments.

    - The Government should modernize its procurement processes to achieve the level of agility demanded by the emerging technology environment. In particular, the Government should consider establishing a special fund that agencies can use to

replace legacy information technology systems[2] that pose unacceptable cybersecurity risks; accelerating agency use of existing funding for small-scale testing or piloting of shared services or new technologies; and supporting the development of dedicated, cross-agency procurement teams that are knowledgeable about forthcoming technologies and skilled in agile processes.

- **Promote and Prepare for IoT Capabilities that Agencies Can Leverage to Advance Their NS/EP Missions.**

  - The Government should direct the Office of Management and Budget to require agencies to: (1) assess and document IoT capabilities that currently support and/or are planned for support of NS/EP functions, considering interconnections and interdependencies that may be introduced; and (2) develop plans to manage security risks created by current and future IoT deployments. The plans should recognize the fast pace of IoT innovation and that some parts of the IoT ecosystem may, at least initially, prove very hard to secure (e.g., due to the number of devices and lack of security standards). As a result, Government plans must be adaptable, and the Government must be able to provide NS/EP services even if IoT functions or capabilities are degraded.

  - The Government should sustain and, where relevant, strengthen investments in facilitating Government and industry coordination to address IoT opportunities and risks, including by: (1) continuing to support public-private partnerships being pursued by the Department of Commerce (DOC);[3] and (2) tasking the DOC to continue advocating for industry-led approaches and consensus-based standards by establishing a Government and industry standing body to collaborate on and leverage the various industry IoT consortia guidelines that are being developed, updated, and maintained to manage IoT deployment risks.

- **Improve Manageability, Security, and Resilience of Current and Future ICT.**

  - As part of its policy and plan for the efficient acquisition and implementation of SDN and NFV in Federal networks, the Government should address the security of SDN/NFV technologies. In particular, the Government should consider SDN/NFV control plane issues as well as other cybersecurity and supply chain security issues relevant to the new technology.

  - The Government should energize public-private initiatives focused on improving identity management.[4] In particular, the Government should require strong, multi-factor authentication for access to Government networks and citizen-facing services. Additionally, the Government may consider serving as a source for the private sector to validate trusted identities, including in the context of biometrics.

[2] The White House. "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[3] National Telecommunications Industry Association (NTIA). "Internet of Things." Accessed on: April 4, 2017. https://www.ntia.doc.gov/category/internet-things.

[4] The White House. "The National Strategy for Trusted Identities in Cyberspace." Accessed on: July 5, 2017. https://obamawhitehouse.archives.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace.

- The Government should facilitate cross-agency efforts to evaluate NS/EP applications for blockchain technology, including the sharing of trusted transactions and other data, such as digital identity or cybersecurity threat information. The use of blockchain will likely be particularly relevant when the integrity of transactions or data is critical. In addition, the Government should facilitate cross-agency efforts to evaluate the potential risks of using or relying on blockchain technology for NS/EP applications.

- **Invest in Government Participation in Global Technology Standards Forums.**[5]

  - 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 centrally coordinate its engagement in global technology standards forums at the executive leadership and interagency levels. In addition, it should develop mechanisms for regular collaboration with the private sector and other governments, enabling strategic prioritization and investments.

Strategic Opportunities:

- **Position the U.S. Workforce to Create, Use, and Manage 21st Century Technology by Investing in Education and Training Programs.**

  - The Government should invest in education and training programs that enable the Government, as well as the broader U.S. workforce, to be prepared to leverage new technologies and lead ongoing innovation. Special attention should be focused on programs that address developments in AI and machine-to-machine communication.

  - The Government should invest in re-training programs and employment services for disciplines that may be affected in the near term by shifting labor needs.

- **Assess New Governance, Legal, and Operational Challenges Resulting from Emerging AI, Autonomous Devices/Systems, and Materials Science Advances.**

  - The Government should drive and/or support research to achieve greater clarity around the impacts of software-based decision-making by autonomous systems, including both military and commercial systems that could impact NS/EP, partnering with the private sector and other critical stakeholders as appropriate.

[5] National Institute of Standards and Technology (NIST). "NISTIR 8074 Volume 1: Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity." Accessed on: July 5, 2017. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf. NIST. "NISTIR 8074 Volume 2: Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity." Accessed on: July 5, 2017. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf. NIST. "Comments on the 8/10/15 Draft NISTIR 8074, Volumes 1 and 2." Accessed on: July 5, 2017. https://www.nist.gov/itl/comments-draft-nistir-8074-volumes-1-and-2.

- The Government should drive and/or support research to achieve greater clarity around the impacts of hardware-based innovations enabled by new meta-materials and materials science advances, partnering with the private sector and other critical stakeholders as appropriate. In doing so, the Government should identify NS/EP risks brought about by the advent of very small sensors, computers, and communications devices or resulting from new capabilities that may be embedded in low-cost, multispectral/hyperspectral sensors.

- **Prepare for the Impact of Quantum Computing, Including its Impact on National Security Information.**

  - The Government should ensure that it is funding and managing the promulgation of quantum-related research and technologies consistent with risk while also contemplating the impact of quantum computing capabilities in the hands of another nation state or a private sector entity. In particular, the Government should review current research and development (R&D) efforts across the ecosystem, taking into account significant efforts underway in the private sector, and determine whether its own R&D efforts are adequately resourced and coordinated. If the Government determines that investment levels need to be increased to support U.S. R&D leadership, then significant engagement with Congress should be pursued. In addition, the Government should consider appropriate controls on precursor technologies for quantum computing, including controls on extreme refrigerants.

  - The Government should focus on the deployment of quantum-resistant encryption and ensure that critical national security information and systems (that will need to remain classified over an extended period of time) are being sufficiently prioritized. In particular, the Government should develop a plan to implement quantum-resistant encryption schemes in a prioritized way, recognizing that deployment may be delayed if cryptographic agility is not sufficiently integrated into relevant technology systems. The Government should also consider the early deployment of hybrid cryptosystems that would combine a new quantum-resistant scheme with an existing, well-studied public-key algorithm, taking into account the lifetime of sensitive information that is currently being generated and that could be recorded and stored for later decryption.

Cross-Technology Imperatives:

- **Establish a Cybersecurity Moonshot Strategy to Fundamentally Transform the Security of our Digital Landscape within a Decade.**

  - The Government should establish cybersecurity as a national strategic imperative, harnessing the collective resources and capabilities of the Government, private industry, and academic community to simplify cybersecurity consumption and delivery models through accelerated research and action in at least four key and interrelated areas: network design, machine learning, automatic orchestration, and quantum computing. In doing so, the Government should recognize the unprecedented but narrow opportunity for change enabled by disruptive

forthcoming technological developments. The Government should also drive accountability for leading the development and implementation of this strategy by designating a senior Government official to lead this cross-Government effort.

- **Institute and Integrate Planning and Preparation for Technology Changes and Landscape Shifts into Existing Cross-Government Efforts.**

  - The Government should institute periodic assessments of disruptive ICT developments by integrating emerging technology-focused scenarios into existing planning exercises, recognizing the pace of ICT developments and the value of regularly considering how the forthcoming environment may shift opportunities and risks. The Government should integrate such future-focused scenarios and planning into existing cross-governmental efforts, such as the Federal Emergency Management Agency's National Level Exercises or the *National Infrastructure Protection Plan*.

  - The Government should foster cross-agency collaboration on technology adoption to lower costs and improve efficiencies and effectiveness by: (1) documenting approaches that address practical scenarios relevant across agencies; and (2) continuing to promote existing incubation efforts and to support technical evaluation labs that help to integrate innovations within functional settings. Examples include programs that promote cross-vendor interoperability at the National Institute of Standards and Technology and that are based on industry partnerships at the National Cybersecurity Center of Excellence.

- **Review Existing NS/EP Public-Private Partnerships to Assess Whether Relevant Stakeholders Are Identified and, to the Extent Warranted, Represented.**

  - 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.[6] 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.

[6] NSTAC. *NSTAC Report to the President on Information and Communications Technology Mobilization.* November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

1.0 INTRODUCTION

In recent years, increasingly rapid innovation and information and communications technologies (ICT) adoption[7] have created new opportunities as well as new challenges. The swift uptake of mobile technologies has facilitated vast advancements in connectivity, supporting a global marketplace while enabling new methods of intrusion or attack. Social media applications have generated new communities that interact in positive and negative ways. The Internet of Things (IoT) is not only enabling incredible efficiencies but also connecting unprotected devices that contribute to record-setting botnets.[8]

Over the next decade, more waves of technological innovation are forthcoming—as are more opportunities and challenges. How the Government and other organizations prepare for these forthcoming waves of innovation will have profound effects on security, prosperity, and society. As discussed below, the Executive Office of the President (EOP) requested that the President's National Security Telecommunications Advisory Committee (NSTAC) study emerging technologies and assess their potential impacts on the Government's national security and emergency preparedness (NS/EP) mission. This report describes the forthcoming technology landscape and incorporates recommendations intended to help the Government prepare for near- and long-term impacts of emerging technologies on the NS/EP mission.

This report is organized as follows. Section 1.0, *Introduction*, provides an overview of the NSTAC tasking that resulted in this study and report as well as an outline of the approach taken by the Subcommittee to carry out that tasking. Section 2.0, *The Future Technology Landscape*, describes the taxonomy used to organize and convey information about the various technologies included within this report, and it also uses graphics to introduce the technologies. Section 3.0, *Technology Discussion*, provides greater detail on each technology, including an explanation of the technology and its potential impacts, both generally and in the NS/EP context. Section 4.0, *Impacts on NS/EP Functions and Missions*, provides a cross-technology assessment of potential impacts to the Government's NS/EP mission. Section 5.0, *Recommendations*, includes high-priority actions, strategic opportunities, and cross-technology imperatives that the Government may consider to prepare for near- and long-term technology developments.

1.1 Scoping and Charge

In December 2015, the EOP requested that the NSTAC study current and emerging ICT and immediate, near-term, and long-term implications of such technologies on NS/EP functions. Therefore, in January 2016, the NSTAC created the Emerging Technologies Strategic Vision (ETSV) Subcommittee, which structured its study in two distinct phases. In Phase I, the ETSV Subcommittee focused on current technologies and recommendations for how the Government can, in the immediate future, better harness them to modernize and mitigate challenges to NS/EP functions. In March 2016, the Subcommittee presented a letter to President Obama and his

[7] Rita McGrath. *The Pace of Technology Adoption is Speeding Up*. Harvard Business Review. November 25, 2013. https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up.

[8] United States Computer Emergency Readiness Team (US-CERT). "Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets." Accessed on: July 5, 2017. https://www.us-cert.gov/ncas/alerts/TA16-288A.

Administration, recommending immediate actions to be taken to enhance Federal cybersecurity risk management and governance of Federal cybersecurity efforts.[9]

The ETSV Subcommittee then began to work on Phase II, focusing on forthcoming innovation and producing this in-depth report for President Trump and his Administration. This report examines emerging technologies and their potential near- and long-term impacts on the Government's NS/EP mission. The NSTAC's goal in undertaking this study and producing this report is to inform the Administration's efforts to determine priorities and formulate policies on modernizing Government operations and preparing for new ICT capabilities.

1.2 Approach

To complete Phase II of the ETSV Subcommittee's study, the NSTAC used several research methods, including receiving briefings and reviewing reports and articles on current and future ICT growth areas. The NSTAC heard from public sector, private sector, and academic experts on a range of both near- and long-term technology developments and how they will impact the Government's NS/EP capabilities and mission.

Overall, the NSTAC:

- Received over 30 briefings from subject matter experts across private industry, academia, and the public sector;
- Reviewed Federal ICT policies, regulations, guidance, and reports, such as the Executive Office of the President's report on *Preparing for the Future of Artificial Intelligence*;
- Reviewed current industry best practices and relevant technology research; and
- Examined academic studies regarding emerging technologies.

The NSTAC focused on examining forthcoming technologies and how the Government can ready both itself and the Nation to benefit from and mitigate the risks of those innovations.

2.0 THE FUTURE TECHNOLOGY LANDSCAPE

The NSTAC's first task was to gain an understanding of the technology that will become relevant during the timeframe addressed in this study (i.e., now to approximately 10 years in the future). From the outset, the picture that emerged was complex and dynamic. The NSTAC encountered a landscape that is changing, but not necessarily in uniform or coherent ways. Some transformation is very pronounced in the private sector but scarcely noticeable in Government. Some technology developments are highly interdependent while others stand in a more competitive relationship. As in a physical landscape, some emerging technologies work to erode established structures while others threaten catastrophic re-ordering of entire environments. Legacy technologies vanish in some contexts and cast a long shadow in others.

[9] NSTAC. *NSTAC Emerging Technologies Strategic Vision (ETSV) Letter to the President.* March 10, 2016. https://www.dhs.gov/sites/default/files/publications/Att%20%201%20-%20NSTAC%20Emerging%20Technologies%20Strategic%20Vision%20%28ETSV%29%20Letter.pdf.

This diversity of characteristics is not the only challenge presented by the future landscape; emerging technologies also vary widely in the degree of certainty with which they can be described. Though most can be described with concrete references to existing or clearly imminent applications, the projection of some technologies beyond a certain point in time tends to produce a more speculative and untethered dialogue, and that inflection point varies for each technology examined.

2.1 Conceptual Maps of Forthcoming Technology

To provide a sense of the relative maturity of various innovations and potential timelines for deployment, this section contains two conceptual maps of emerging technologies. Multiple graphics are included to help illustrate that different approaches exist to capture the expected emergence of technologies, and each of them is limited in various ways. Figure 2.1, provided by an NSTAC briefer, captures the emergence of a range of technologies over time, highlighting maturity of expectations around a given technology. It goes beyond but does not comprehensively cover all of the technologies discussed in this ETSV report, though there is significant overlap in what it conveys and what is covered in the report.

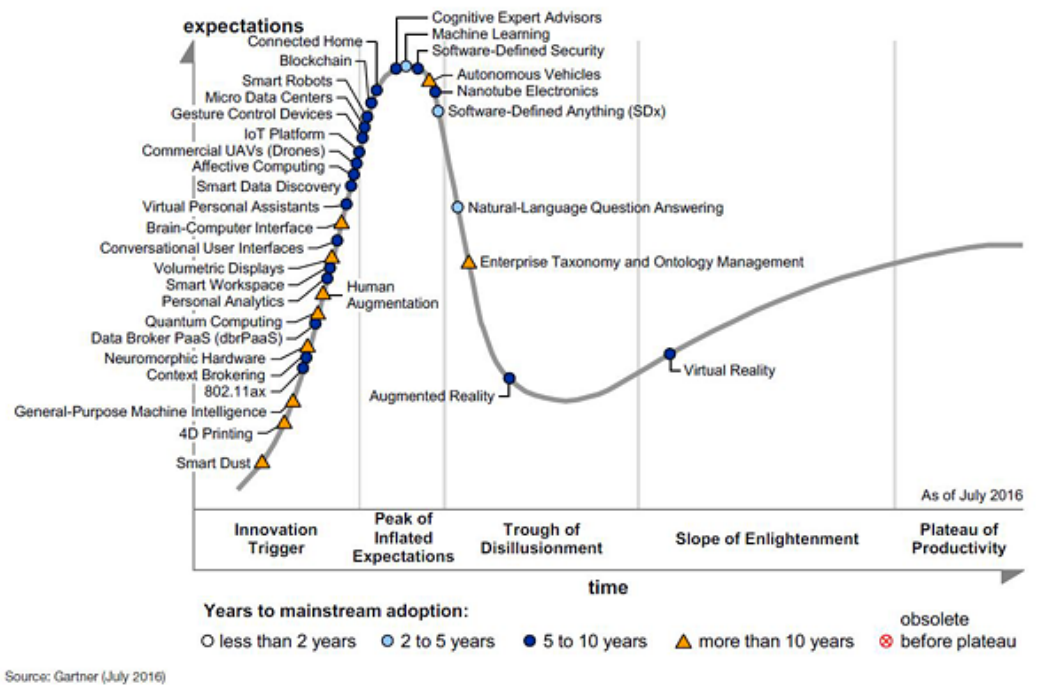

Figure 2.1. Common Developmental Stages Observed in Emerging Technologies[10]

Figure 2.2 comprehensively covers each of the technologies discussed below and introduces the trends taxonomy that is used within this report. The technologies are organized according to four trends (which are described below), the estimated time it will take them to produce a significant NS/EP mission impact, and their relative maturity of development. Notably, while both Figure

[10] Gartner, Incorporated. "Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage." August 16, 2016. https://www.gartner.com/newsroom/id/3412017.

2.1 and Figure 2.2 highlight the relative maturity of technologies, these technologies are in a constant state of development that will likely be punctuated by iterative deployments. Some, like blockchain, are categorized as near term but may evolve significantly over the long term.

Within Figure 2.2, the dimensions of maturity of technology and time to impact are considered, but the degree or extent of potential impacts on the Government's NS/EP mission is not represented. As such, there is a correlation between maturity of technology and time to impact, but technologies closer to the bottom right corner are not necessarily more important or impactful for the Government's NS/EP mission than technologies closer to the top left corner. For instance, as described below, quantum computing will have an enormous impact on the Government's NS/EP mission, potentially even outpacing the cumulative impact of many near-term transformative technologies. However, Figure 2.2 does not depict this dimension of degree or extent of impacts due to the complexity of visually representing such nuanced and variable information. Rather, the text below gives a sense of the range of potential impacts of each technology, and the report's recommendations, which are tied to technologies' designation as near- or long-term transformative, are not arranged or ranked in order of importance.

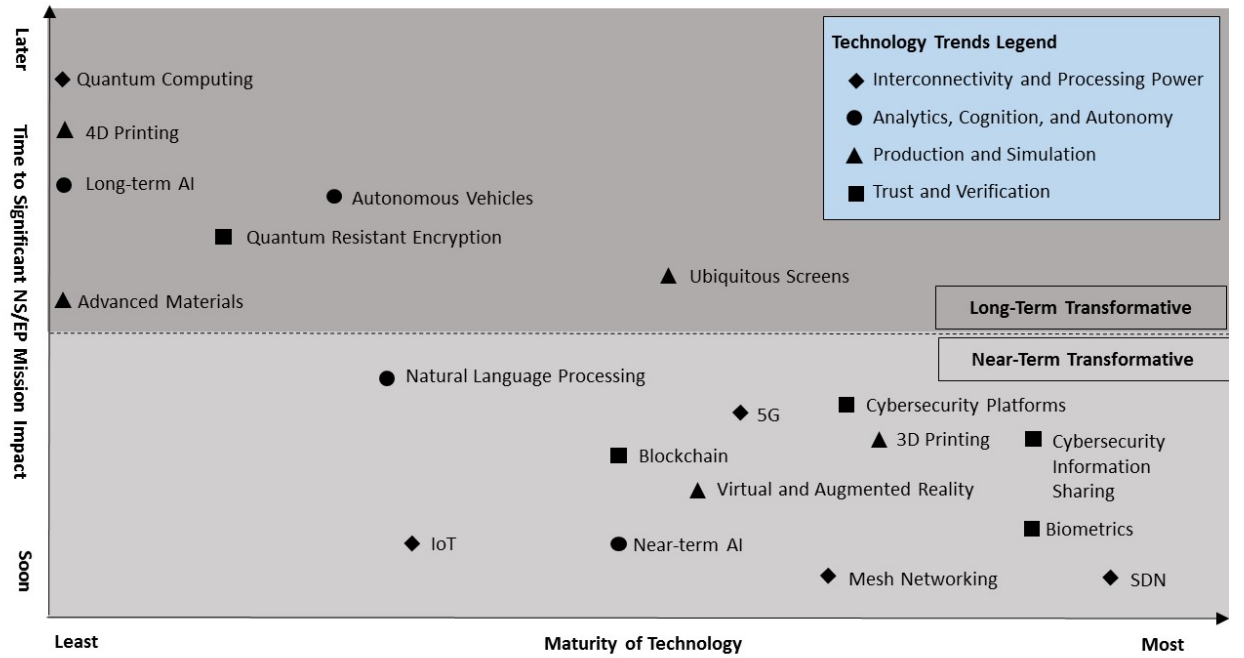

Figure 2.2. ETSV Report Technologies

2.2 Taxonomy for Forthcoming Technology

The NSTAC's task was to examine the potential effects of emerging technologies on the NS/EP mission and to provide actionable recommendations to the President on how to best leverage or mitigate those effects. To help achieve this, the NSTAC first developed a taxonomy to enable meaningful interpretation of the landscape. The NSTAC's taxonomy consists of two distinct sorting tools: categories and trends. In Section 2.3, *Two Technology Categories*, two categories are described: (1) technology that is well developed and is currently being or will soon be deployed; and (2) technology further off on the horizon but in some cases even more

dramatically transformative. Then, in Section 2.4, *Four Technology Trends,* four trends, or changes affecting a particular area of technology, are described.

The NSTAC's hope is that, by applying both tools, a policymaker will be able to assess immediacy, effects, and interdependencies for any given technology. For example, the application of categories should provide insight into the expected deployment of a technology over time. Similarly, the identified trends should enable policymakers to gain some sense of the technological interdependencies and related opportunities or challenges that may exist.

As in any taxonomy, there are inherent limitations. The classification of items is intended as an interpretative tool that should aid but not constrain policy discussions. The NSTAC is also cognizant of the accelerated timescale in the emergent technology environment. The NSTAC received most of its technical briefings in the summer and fall of 2016; there have undoubtedly been relevant technical developments, even in the few intervening months.

2.3 Two Technology Categories

Near-Term Transformative:

The first category consists of technologies that the NSTAC found to be currently transforming or set to transform ICT architecture or functionality. Specifically, these technologies will impact the Government's NS/EP mission over the next one-to-five years. They are now being deployed in the private sector, will be deployed in the very near term, or, while not fully mature, are well along in their development. The current deployment wave is either clearly defined and technical standards are already substantially complete, or first generation examples of these technologies are appearing in the commercial space, with next generation advances not constrained by any foreseeable technical limits. However, technologies in the near-term transformative category are not generally present in the Government space, and they do not seem to have exercised much influence on the architecture of Government systems. Still, the introduction of near-term transformative category technologies into Government operations is clearly foreseeable, and many of them may be considered, to some extent, in the next cycle of Government procurement.

Examples of near-term transformative technologies include software-defined networking (SDN) and related virtualization architectures. SDN technologies are already being deployed in the private sector, particularly in the telecommunications sector, and are integrated into the current generation of ICT offerings. The near-term transformative category also includes many IoT technologies, 5G, 3D printing, biometrics, and blockchain.

Long-Term Transformative:

The second category consists of technologies that will fundamentally alter multiple disciplines and environments within ICT in ways that cannot be accurately described within the current technical vocabulary. Many represent a tectonic shift in the environment, and they will necessitate the development of new, foundational concepts in computer science and related disciplines; these technologies may also re-order the relationships between and among computer science, materials science, biology, and mathematics. However, the impact of these technologies on the Government's NS/EP mission will be delayed; significant deployment is at least five years out, and in many cases, likely more. For the most part, long-term transformative technologies

exist only in the research environment, and, even there, they are often not yet in a workable form. Still, key advances have been made in the enabling science for these technologies—to the extent that they have moved from the purely speculative to the reasonably expected.

For most of these technologies, the estimated time of arrival or widespread deployment remains somewhat unclear, but there is general agreement that these technologies are reliably present over the horizon. For the Government, the principal challenges are to appropriately manage research efforts, particularly where these technologies would have a very direct impact on NS/EP equities, and to prepare for future deployment. Examples of long-term transformative technologies are quantum computing and advanced materials, including active nanotechnology.

2.4 Four Technology Trends

In today's interconnected world, few technologies are developed in a vacuum. As technologies emerge and evolve, they may also advance, delay, or alter the development of other technologies. To demonstrate these links or dependencies, this section describes four thematic technology trends: interconnectivity and processing power; analytics, cognition, and autonomy; production and simulation; and trust and verification. Each trend builds on the foundation established by the one before it, resulting in a technology stack that works both conceptually and physically. For example, interconnectivity and processing power developments have been foundational to analytics, cognition, and autonomy developments, enabling sufficient data, storage, and computing power to generate leaps forward in artificial intelligence (AI) capabilities.

In addition, the trends highlight the major functional impacts of forthcoming technology developments by bringing related technologies or capabilities together under one thematic umbrella. For example, the thematic grouping of interconnectivity and processing power brings together a range of near- and long-term technologies and approaches that may drive advances in this trend, including through fundamentally different approaches.

However, these overarching trends are not absolute; rather, some technologies have functions or impacts that bridge or cut across multiple trends. For instance, quantum computing will not only advance processing power capabilities but also significantly impact trust and verification by breaking leading encryption algorithms. Likewise, interconnectivity is foundational to IoT, but many IoT devices will also enable and embed analytics, cognition, and autonomy. Recognizing these tensions, the NSTAC still found that the thematic grouping of trends usefully highlights the functional impacts of and interdependencies between forthcoming technology developments.

Interconnectivity and Processing Power:

Over the last two decades, billions of people and things—including not only personal computers but also mobile devices, wearable devices, home appliances, and sensors—have been connecting to networks and to each other. All of those devices have been powered in accordance with Moore's Law, [11] as electronics have become less expensive, more compact, and better performing due to consistent improvement of processors. Meanwhile, connections between an ever-

[11] Moore's Law states that technology continually expands at an exponential and measurable rate or, more commonly, that computer power doubles every two years at the same cost. The Economist. "Technology Quarterly: After Moore's Law," March 12, 2016. Available at: http://www.economist.com/technology-quarterly/2016-03-12/after-moores-law.

increasing number of devices have been supported by wireless technologies (e.g., 4G), Internet Protocol (IP) version 6 (IPv6), and other developments that have increased the speed, availability, and bandwidth of network connections.

The next advancements in this continuing evolution, including SDN, 5G, and wireless mesh networking, will support the forthcoming influx of billions of IoT endpoints that will require that communication and functionality become faster, cheaper, more powerful, more dynamic, and more resilient. In addition, this trend includes quantum computing, which is one of numerous potential computing architectures that will likely emerge and transcend the speed of evolution within processing technology currently observed by Moore's Law.

Analytics, Cognition, and Autonomy:

In 2016, future technologist Kevin Kelly wrote that applied AI will become available for and incorporated into everything, just like electricity was over 100 years ago—a process he called cognifying.[12] In 2014, Erik Brynjolfsson and Andrew McAfee offered another metaphor: "Now comes the second machine age. Computers and other digital advances are doing for mental power…what the steam engine and its descendants did for muscle power."[13] As with both electricity and steam engines, the impact of analytics, cognition, and autonomy will be extraordinary and far-reaching, integrating capabilities and enabling advances across a range of domains. This trend of analytics, cognition, and autonomy captures those potential developments as well as their near-term manifestations, including forms of AI that are already being commercialized today. Ultimately, this trend captures new and forthcoming abilities to process, make sense of, and apply vast amounts of information to resolve questions, discover and share insights, and act—both with and without humans.

Production and Simulation:

Society is amidst a major shift from an industrial age to an information age. We are shifting from analog to digital, from entirely physical to a mix of physical and virtual. Moreover, what is physically possible is shifting as advanced materials can increasingly be integrated into everyday objects and new, nanoscale devices. These shifts are manifesting in a range of ways, including how we consume and share information, how products or services can be customized for particular users, and what qualifies as an ICT device.

This trend captures forthcoming changes in how we produce objects, simulate and analyze future production, and experience and interact in both the real and simulated world. These changes will likely enable lower cost, more efficient, and more iterative development; greater potential for shared resources and more interactive learning; more flexibility in environmental requirements; and enhanced interconnectivity and analytic capabilities. Developments captured within this trend include ubiquitous screens, virtual reality (VR) and augmented reality (AR), 3D and 4D printing, and advanced materials, including active nanotechnology.

[12] Kevin Kelly. *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (2016).

[13] Erik Brynjolfsson and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (2014).

Trust and Verification

With ubiquitous connectivity and technology integrated into nearly every aspect of how we work, play, and interact, how we enable trusted communications and verify the identity of people and devices, the provenance of software, and the integrity of data will become increasingly important. As such, amidst broader ecosystem changes, many of which will result in new security benefits and risks, there are also forthcoming developments around technologies that focus on furthering trust and methods of verification. Specifically, there are new and evolving ways of ensuring the confidentiality, integrity, and availability of information and communication, regardless of the platform or activity.

In the near term, technologies and risk management processes, including cybersecurity platforms and information sharing, will mitigate risks and evolve defensive tactics. Biometric information will be increasingly used to verify identities, including through mobile and other devices. In addition, technologies that are especially relevant for decentralized systems, including blockchain, will increase in relevance. Over the long term, technologies that are responsive to new risks, including quantum-resistant encryption, will be standardized and deployed.

3.0 TECHNOLOGY DISCUSSION

This section describes the emerging technologies that the NSTAC has studied and introduces the potential impacts of such technologies on the Government's NS/EP mission. The section is organized by technology trends (i.e., interconnectivity and processing power; production and simulation; analytics, cognition, and autonomy; and trust and verification), and within each trend, categories (i.e., near-term transformative and long-term transformative) are used to describe each distinct technology or area of forthcoming technologies.

For each emerging technology, this section provides a brief introduction to the technology, a discussion of its potential range of impacts, and an explanation of the potential benefits and risks of the technology as it relates to the Government's NS/EP mission. In Section 4.0, a cross-technology and cross-trend overview of NS/EP impacts is also provided.

3.1 Interconnectivity and Processing Power

There is a clear trend, cutting across multiple technologies at different stages of development, toward increased interconnectivity and processing power in ICT networks. Interconnectivity is manifest both in the evolution of network design (toward more virtualized and distributed architectures) and in the rapid deployment of sensors and communications capabilities to physical devices (IoT). Explosive growth in processing power has been less evident in recent years, but with the expected arrival of fundamentally disruptive computing architectures that may slip the bounds of Moore's Law,[14] the concept of

Moore's Law 2.0: There will not be a single Moore's Law in the future but a variety of them, depending upon computational architecture, software, and application. New computing architectures include:

- Quantum
- Neuromorphic
- Graphene
- Optical
- DNA

[14] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee*. June 14, 2016.

processing power is going to expand. In particular, in the context of these fundamentally disruptive computing architectures, this report focuses on quantum computing, an architecture that will have profound impacts not only on processing power but also on other trends discussed within this report, including analytics, cognition, and autonomy as well as trust and verification.

Technologies discussed within this interconnectivity and processing power trend include:

- SDN;
- IoT;
- 5G;
- Wireless mesh networking; and
- Quantum computing.

Figure 3.1 highlights these technologies as they were represented above in Figure 2.2.

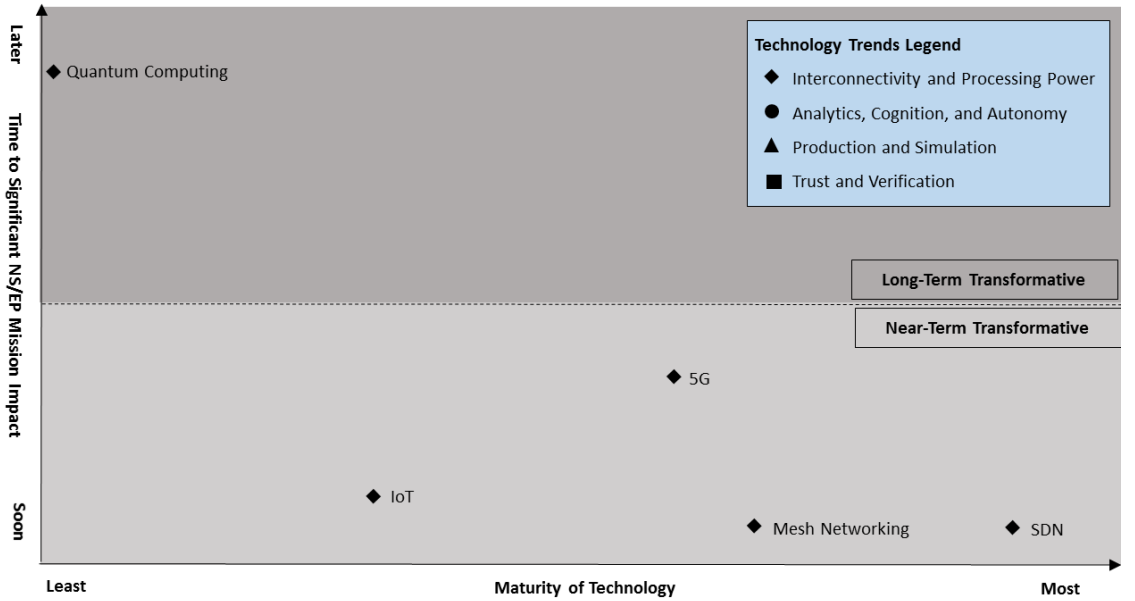

Figure 3.1. Interconnectivity and Processing Power

3.1.1: Software-Defined Networking (Near-Term Transformative)

Introduction:

SDN and NFV represent an ongoing shift occurring in networking away from legacy technologies based upon hardware to software-based networks that leverage standard, off-the-shelf or commodity-based hardware. This shift is structurally transforming the ICT ecosystem and allowing networks to become more flexible and adaptive. It began with the arrival of cloud computing, an enabling technology that disrupted the traditional architecture of an enterprise network. Further detail on cloud computing as background for the emergence of SDN/NFV is included in the box below.

SDN decouples a network's control plane and data plane as well as its network functions from dedicated hardware. As a result, control plane functions (i.e., decisions about where traffic is sent) can run on a virtual machine, enabling more dynamic access to and administration of a more flexible network.

What is SDN?

Cloud computing: A precursor to and enabling technology for SDN

Before cloud computing, enterprises (whether in the private sector or Government) generally maintained their networks with their own staff and in their own facilities. Enterprise IT staff purchased and configured equipment, maintained hardware and software, and were responsible for securing the enterprise's data and network. A typical network consisted of hardware dedicated to specific functions: routers, Web servers, storage arrays, e-mail servers, switches, etc. The extent to which these devices (and their attendant software) were maintained, updated, and secured depended largely on the level of expertise and resources available to the enterprise's IT staff. The availability of data and the ability to restore data to the system likewise rested on internal IT practices like proper redundancy in network design and routine data archiving. Where IT activities were not properly resourced, the network's security, integrity, and efficiency could all be put at risk.

The arrival of cloud computing architecture(s) in the mid-2000s promised to address some of the inherent weaknesses and dependencies in enterprise networks. The idea behind cloud computing was to centralize resources, operating computing hardware in large data centers to which enterprise users would connect via broadband or other high speed facilities. Initially, the data centers simply offered space and environmental controls: the enterprise was essentially moving its network hardware to a different location (i.e., colocation). Over time, cloud vendors began to offer services using hardware and software they had installed in their data centers; this model went through various iterations and was sometimes referred to as computing as a service. The next evolution in cloud services was to offer an environment (still contained within a data center) that allowed the customer to remotely configure hardware/software assets within the data center to emulate the required network components. The customer could thus create virtual machines within the customer's space in the data center, and the customers could also alter the number and configuration of these machines using a control interface (often referred to as a hypervisor).

Basic functional components of ICT are shifting first into a cloud-based environment and from a physical cloud into a virtual cloud. Cloud computing's potential efficiencies and flexibility have driven widespread adoption of the technology in the private sector, and Government is beginning to follow suit. In 2011, the Federal Government developed a unified strategy for migration to the cloud, and in 2013, the NSTAC examined the cybersecurity implications of the Government's use of cloud computing. The report stressed the need to properly secure the new infrastructure through creation of effective cybersecurity measures and the development of a culture of cybersecurity among the now more dispersed elements of the Government's IT infrastructure. Most relevant to this report, the NSTAC also urged the Federal Government to take advantage of this shift in technology to get ahead of the cybersecurity challenges and leverage the opportunities it presents.

Cloud Computing, Government Adoption, and NSTAC[15,16,17,18,19]

---

[15] Vivek Kundra. *Federal Cloud Computing Strategy*. February 8, 2011. https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

[16] Federal Risk and Authorization Management Program. "About Us." Accessed on: April 10, 2017. https://www.fedramp.gov/about-us/about/.

[17] Steven VanRoekel. *Security Authorization of Information Systems in Cloud Computing Environments* [Memorandum]. December 8, 2011. https://www.fismacenter.com/fedrampmemo.pdf.

[18] NSTAC. *NSTAC Report to the President on Cloud Computing*. May 15, 2012. https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf.

[19] Please refer to Section 5.0, *Recommendations*, for more information.

SDN is an umbrella term encompassing several network technologies aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of a cloud computing data center. Key attributes and technologies include functional separation, which decouples the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that move traffic to the selected destination (the data plane); and NFV, which decouples network functions from dedicated hardware devices and allows network services that are now carried out by routers, firewalls, load balancers, and other dedicated hardware devices to be hosted on virtual machines.[20,21] In conventional networking, the control plane and the data plane are implemented in the firmware of routers and switches; the combination of functional separation and network virtualization means that control plane functions can run on a virtual machine. Moreover, in decoupling the data and control planes and implementing the control plane in software, SDN enables dynamic access to and administration of more flexible networks.

Discussion:

The private sector is now seeing architectural shifts similar to cloud computing for enterprise networks occur in large scale ICT networks; traditional, hardware-based switching capacity and other common network elements are beginning to migrate to the cloud. Just as shifting enterprise networks and computing resources to cloud-based environments was precipitated in part by various limitations of enterprise IT, there are a variety of computing trends driving the need for a new paradigm for large scale ICT networks. In particular, there is an increasing need for flexibility and quick capacity to scale with surges in demand. For example, applications require flexible traffic management and access to bandwidth on demand, changing traffic patterns; bring your own device trends require networks that are more flexible and enable different security capabilities; and the rise of cloud services and big data result in constant demand, driving a need for additional capacity and more flexible connectivity.

While this movement is essentially taking the central features of cloud computing and expanding them beyond the typical data center/enterprise arrangement into core ICT networks, there is one key difference. Unlike existing cloud technologies, SDN is not simply an option for standard enterprise architectures; it also is changing how communications networks are architected. For example, the NSTAC found that telecommunications providers are already deploying virtual switches as part of the next evolution in the public switched telephone network (PSTN). These deployments are part of a process that could eventually erase the distinctions between the legacy PSTN and the backbone of the Internet. Thus, a major communications infrastructure is undergoing real transformation.

This next evolution will enable SDNs that span multiple physical locations and virtualization capabilities that encompass all functions previously assigned to specific hardware. These assets will be configured via a control plane (like the hypervisor in a cloud data center, but much larger in scope), which enables network control to be decoupled from the underlying data plane and to be directly programmable. A user could procure a virtual area or slice of the architecture and use

[20] Margaret Rouse. "Software Defined Networking (SDN)." August 2015. http://searchsdn.techtarget.com/definition/software-defined-networking-SDN).

[21] Margaret Rouse. “Network Function Virtualizations (NFV).” March 2016. http://searchsdn.techtarget.com/definition/network-functions-virtualization-NFV.

it to create a network, adding virtual machines of all types and modifying the size and features of the network as needed. A network administrator could shape traffic from a centralized control console—exercising significant control and prioritizing, de-prioritizing, or blocking specific types of packets—without having to touch individual switches. Functional separation and network function virtualization (NFV) make it possible to implement changes to the network in near real time, removing the time and expense of re-deploying physical infrastructure.

Figure 3.2 is a basic diagram of the components of an SDN:

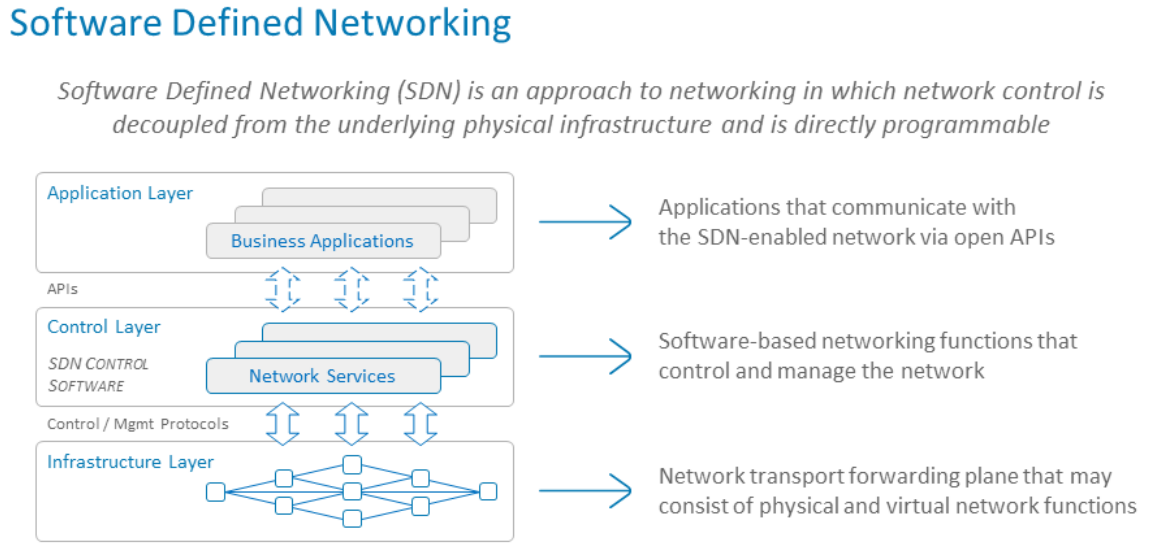

Figure 3.2. Software-Defined Networking

The diagram below, Figure 3.3, illustrates how traditional network appliances, largely comprised of specialized, non-commodity hardware and physical appliances, can be replicated using NFV.

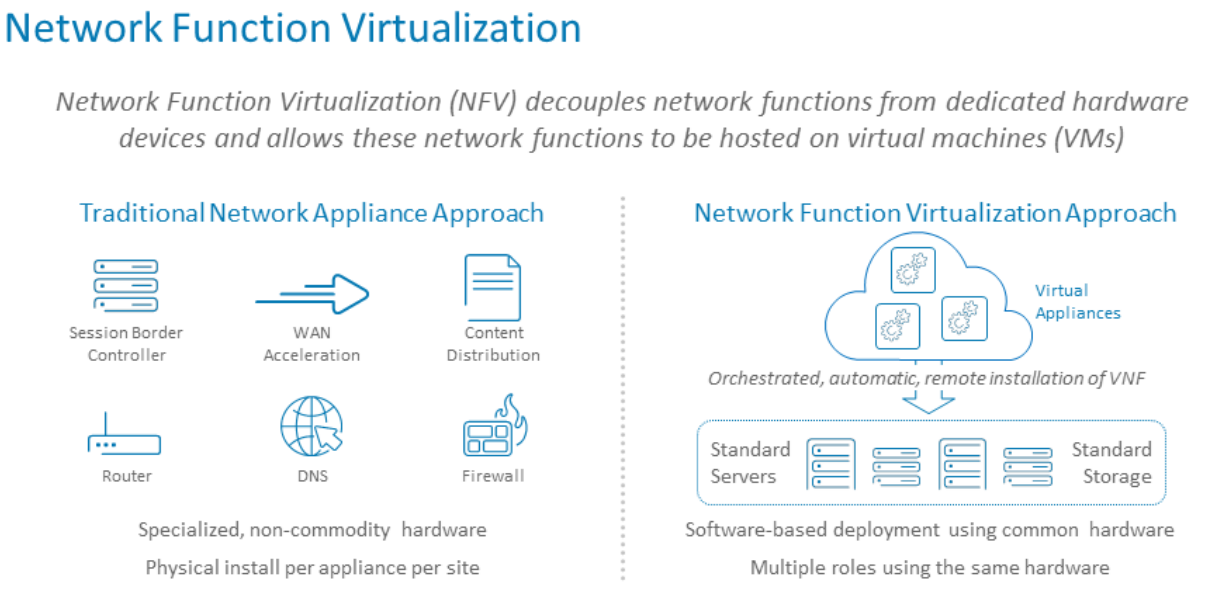

Figure 3.3. Network Function Virtualization

Beyond private sector efforts and applications of these technologies, significant experimentation with SDN and NFV is currently underway at the Global Environment for Network Innovation (GENI),[22] a National Science Foundation (NSF)-supported[23] virtual laboratory on which the NSTAC was briefed. GENI acts as a U.S.-based testbed for SDN and NFV. Notably, similar testbeds also exist in other countries, and some, including China, are also deploying fully functional commercial versions of GENI.

SDN and NFV offer substantial benefits to network operators, and chief among these is the flexibility of virtual design. It will soon be possible to create and configure networks in a virtual space, essentially untied to any specific hardware infrastructure. Since all functional components of an SDN are software, installation and re-configuration will no longer be dependent upon a specific physical component. A network can be created, altered, and dismantled virtually, resting on completely fungible and widely available hardware assets. The nature of the network is also defined by the software: it could be the operating network of a particular enterprise, a dedicated telecommunications network, a distributed storage environment, etc. While some SDNs will likely be more persistent than others, the technology offers the promise of networks freed from the constraints of a dedicated physical architecture. Network owners would no longer have to invest in function-specific hardware or commit to vendor-defined specifications. Data centers and cloud facilities would become much simpler and more generic platforms with network operators buying access to those platforms to create functional networks.

SDN also allows for a major transformation in security architecture; a more flexible, responsive environment and more effective cybersecurity strategies can be deployed. There are a wide variety of security benefits of SDN, ranging from security by design, where security is built into the design of SDN architecture from day one, to streamlined security add-ons and patching. The following are some of the security benefits of SDN:

- Centralized SDN Security Control: SDN controllers centralize security management decisions while also enabling distributed enforcement.
- Security by Design: Redesign of network infrastructure with SDN and NFV allows for security to be embedded at the earliest stages.
- Add-On Security Protections: SDN enables on-demand, real-time provisioning of add-on security functionality for customers.
- Defense in Depth Architecture: Virtualization enables multivendor, defense-in-depth security chain architectures.
- Streamlined Security Patching: SDN applications, common infrastructure, and SDN inventory streamline the security patch process.

[22] GENI. "What is GENI?" Access on: June 19, 2017. http://www.geni.net/.
[23] NSF. "Global Environment for Networking Innovations (GENI)." Accessed on: June 19, 2017. https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=501055.

- Improved Incident Response: SDN improves incident response due to the simpler restoration of common virtualized infrastructure.

- Distributed Denial of Service (DDoS) Resilience: SDN enables live-scaled expansion to absorb DDoS attacks in real time.

- Perimeter Independence: Cloud-hosted infrastructure can be protected with virtual security that is independent of the enterprise perimeter.

Perimeter independence is a significant potential benefit; in short, SDN can be used to create virtual perimeters or micro-segmentation to enhance enterprise security architectures. Traditional perimeter security like physical firewalls are not sufficient. Once they are breached, entire segments can be compromised, and most traffic resides inside rather than outside the network perimeter. SDN allows security to shift from a traditional perimeter security model (e.g., a firewall) to having embedded, logically separated (rather than physically separated) cloud micro-perimeters that function more like a security wrapper around each instance of various data sets. This can enhance enterprise security by enabling policy management to be linked to specific asset or data sets.

Below, Figure 3.4 illustrates a traditional enterprise perimeter and how that model has changed over time. The need to share services and data with suppliers, vendors, and remote workers has led to a weakening of perimeter walls, and issues such as misconfigurations and firewall exceptions have weakened security. This has made it exceedingly difficult to rely on a perimeter defense model as there always appear to be some exceptions, and, in large enterprises, attackers can find means to utilize those exceptions to get through the perimeter and gain access to important assets. Further, relying upon a single perimeter can potentially allow an attacker that gains access to one system to roam freely across an enterprise.

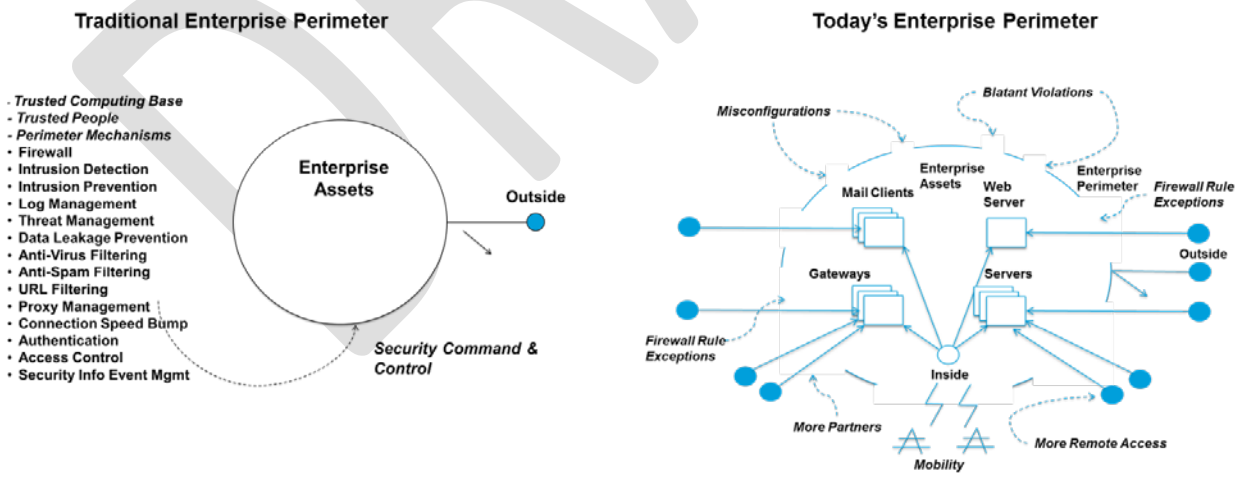

Figure 3.4. Traditional Enterprise Perimeter Versus Today's Enterprise Perimeter

SDN can address this challenge by allowing an enterprise to distribute security and create multiple smaller security rings, protecting classes of assets. This concept is illustrated in Figure 3.5, which shows security rings made with virtualized security components instead of physical appliances, protecting the assets in each ring. Combined with strong authentication, the

enterprise can utilize this architecture to more quickly respond to an attack or intrusion by isolating the issue to a specific ring and/or quarantining the infected assets from the rest of the enterprise network. Thus, the enterprise can become more resilient and have a quicker response to security incidents.

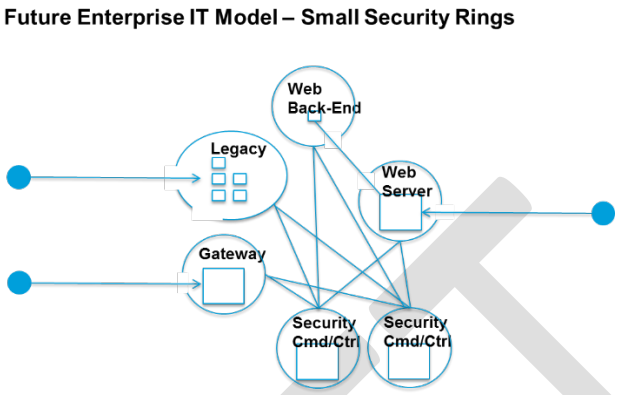

Figure 3.5. Future Enterprise IT Model – Small Security Rings

In addition to potential security benefits, however, SDN also poses security challenges and potentially disruptive effects on cybersecurity. The primary SDN security concerns expressed by NSTAC briefers revolve around two fundamental issues: security of the controller and supply chain security. First, SDN relies upon the controller in its architecture, similar to a hypervisor in a cloud computing architecture, to control various components of the network. Because this represents a shared control plane, a successful attack could proliferate rapidly across shared architecture. Moreover, SDN/virtualization requires the existence of more software than previous security solutions, and software may present more opportunity for bugs or malware to be introduced into the environment. In addition, given the centralization of control with SDN, there is increased risk that if the central controller has a software vulnerability issue, then the impact could be dispersed across the entire network—in other words, the very flexibility offered by SDN/virtualization to network owners could be exploited by attackers. For example, an attacker could quickly create a virtual command and control network and then disassemble it as soon as an attack is successfully launched. As such, there is an acute need to have security controls at each layer, and establishing a secure architecture with a significant barrier to accessing the SDN controller is critical to preventing it from being used as part of an attack.

Second, the use of generic and plentiful hardware components, which are likely to be manufactured at a low cost, and open source software in SDN raises concerns about supply chains and embedded malware. This means that it is critical to secure the SDN controller and overall architecture. Many of the security concepts that are necessary to secure SDN/NFV are similar to those in other cloud computing architectures.

The implications of SDN and virtualization technology will be significant not only for network operators but also for hardware manufacturers, cloud providers, and data centers. The shared nature of SDN platforms means that defensive measures could be propagated quickly through large environments. The move away from function-specific hardware could also simplify the coordination of security tools and facilitate a more integrated security approach. These benefits will be realized only if the adopters of SDN and virtualization leverage the opportunity to deploy

a purpose-built SDN cybersecurity strategy along with the new technology. The opportunity will be lost if legacy practices are simply imported into the new environment.

NS/EP Impacts:

In the NS/EP context, SDN and virtualization technology will have a similarly two-edged effect. With key networks (telecommunications, financial networks, industrial control systems) becoming separate from the traditional physical infrastructure, SDN and virtualization may enable much quicker recovery from disruptive events. After a catastrophic event, key networks could be rebuilt virtually, bypassing assets destroyed in affected areas. Responders also could construct temporary, special purpose networks out of available assets. In the case of predictable events, like weather emergencies, network operators could leverage SDN capabilities to move assets out of harm's way. Fully realized, SDN and virtualization could significantly enhance the resiliency of critical networks and become an important NS/EP tool.

These enhancements, however, come at a cost to some NS/EP equities. The flexibility of SDN and virtualization technology will limit the ability of NS/EP planners to associate physical locations with critical ICT infrastructure. At present, we tend to view the 16 designated critical infrastructures as distinct systems with identifiable physical assets. For each infrastructure, planners identify key facilities, switches, routers, interdependencies, and connections. SDN could make this much less possible. With key assets in networks existing only as software distributed over a generic physical platform, it will be much harder to assess where the assets that need elevated protection are at any given time. Similarly, it will be more difficult to assess the true impact when a physical ICT asset is destroyed since responders may not be able to identify all the software hosted there. The various critical infrastructures may themselves become less distinct, as they all begin to leverage common physical assets to build virtual networks. In addition, supply chain security and broader cybersecurity challenges should be considered as the Government deploys these technologies.

The Government will likely be deploying at least some SDN and virtualization technologies in the near term. This NSTAC study demonstrates that successful deployment will require a considered, Government-wide plan, a commitment to seize the opportunity for implementing an effective cybersecurity strategy, and a careful examination of how to adjust NS/EP and critical infrastructure protection activities to the new technical environment.

Key Concepts	NS/EP Benefits	NS/EP Risks
Networking technologies decouple the control and data plane as well as network functions from dedicated hardware, enabling flexibility in network design, access, and management	• Temporary, special-purpose networks could be constructed for emergency response • Key networks could be rebuilt virtually, bypassing destroyed assets, for quick network recovery • Greater virtual redundancy and resource shifting, increasing resilience	• Planning challenges (e.g., identifying critical infrastructure) • Response challenges (e.g., assessing impact of a destroyed physical asset) • Security challenges (e.g., control plane, supply chain)

3.1.2: Internet of Things (Near-Term Transformative)

Introduction:

Many different industries are incorporating IoT features into their products, and a variety of IoT devices are now entering the market. This wide-ranging deployment of IoT devices represents a broad expansion of the ICT architecture in at least two consistent ways. First, IoT will vastly increase the number of devices that connect to the Internet, and those connected devices will generate enormous amounts of data. Second, IoT devices will increasingly be used to monitor and control the physical environment. While the deployment of IoT has already begun, it is likely to accelerate in the near term with the support of ubiquitous networks and the promise of more robust data analytics and greater operational efficiency.

> IoT refers to a significant range of technologies and devices that sense information, communicate it to the Internet or other networks, and, in some cases, act on that information. These "smart" devices are increasingly being used to communicate and process quantities and types of information that have never been captured before and to respond automatically to improve industrial processes, public services, and the well-being of individual consumers.
>
> **What is IoT?** [24], [25]

The arrival of IoT renders the ICT ecosystem far more complex, especially as the technology cuts across industry sectors and governmental jurisdictions. Governments and regulators are just beginning to consider the complex issues surrounding regulation, security, and standards-setting for IoT. As such, while the NS/EP benefits of IoT are considerable, it is also apparent that the security challenges posed by rapid deployment and easy connection are equally daunting.

---

[24] Government Accountability Office. *Technology Assessment: Internet of Things Status and Implications of an Increasingly Connected World*. May 2017. https://www.gao.gov/assets/690/684590.pdf.

[25] NSTAC. *NSTAC Report to the President on the Internet of Things*. November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf. As defined by the report: "What is IoT? A decentralized network of objects, applications, and services that:

- Are connected to the Internet or another network (e.g., a corporate network);
- Sense, log, interpret, communicate, process, and act on a variety of information; and
- Have some type of kinetic impact on the physical world, either directly or through a mechanical device to which they are connected.

These objects range from small sensors on consumer devices to sophisticated computers in industrial control systems?"

Discussion:

The period during which the NSTAC conducted its study saw IoT move significantly from a coming attraction to a tangible reality. The NSTAC watched the first major DDoS attacks leverage IoT devices to successfully compromise large swaths of the Internet; the attacks illustrated not only how much IoT is already deployed but also the lack of basic security features in many existing IoT devices. Concern about vulnerabilities in IoT drove the development of new IoT-related cybersecurity principles[26] and an initial approach to define the Government's role in addressing those challenges from a strategic perspective.[27] Outside of the Government, there has been robust discussion of the challenges presented by and opportunity to address security for IoT among multiple stakeholders, including civil society, academia, and industry.[28]

The IoT-related material presented to the NSTAC was organized around two themes: the first was that IoT would bring substantial changes to the ICT architecture by interconnecting IT and operational technology (which would have security implications); and the second was that IoT could greatly increase the functionality of connected systems and sensors, providing new insights on their use, improving how they are operated, and enhancing situational awareness and response capabilities in emergency situations. Since many forms of IoT technology are already being deployed and some are rapidly maturing, most of the NSTAC's discussions centered on how the Government should position itself with respect to the technology. Specifically, the NSTAC considered how the Government should address relevant cybersecurity issues and prepare to properly leverage (in the NS/EP context) the capabilities offered by fully deployed IoT. In doing so, the NSTAC both absorbed new briefings and reports and leveraged its previous work on IoT, which was captured in the *NSTAC Report to the President on the Internet of Things.*[29]

The architectural implications of IoT are rooted in its enormous expansion of the Internet through the addition of a nearly unimaginable numbers of sensors, control devices, and functional objects. Among NSTAC briefers, there was broad consensus that the population of IoT devices will exceed 20 billion within the next three years, and some even suggested that such estimates are conservative given the already observed deployment of IoT. These devices, together with their network connections and the data they produce, will significantly enlarge the overall ICT environment. The space for this expansion has already been created by the transition to newer Internet Protocol (IP) addressing protocols (IP version 4 to IP version 6), which expands by a factor of 10^{28} the number of available IP addresses.[30]

---

[26] Department of Homeland Security. *Strategic Principles For Securing The Internet Of Things (IoT).* November 15, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

[27] National Telecommunications & Information Administration (NTIA). *Fostering the Advancement of the Internet of Things.* January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[28] Deloitte. *Wireless Connectivity Fuels Industry Growth and Innovation in Energy, Health, Public Safety, and Transportation.* January 2017. http://www.ctia.org/docs/default-source/default-document-library/deloitte_20170119.pdf.

[29] NSTAC. *NSTAC Report to the President on the Internet of Things.* November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

[30] IBM Knowledge Base. "Comparison of IPV4 and IPV6." Accessed on April 7, 2017. https://www.ibm.com/support/knowledgecenter/ssw_i5_54/rzai2/rzai2compipv4ipv6.htm#rzai2compipv4ipv6__compaddress.

This enlargement will complete a transformation of the Internet into an ecosystem in which machine-to-machine communication may dwarf human-generated content. Multiple NSTAC briefers stressed that the Internet has rapidly evolved from a system primarily designed to connect humans into one that largely, or even primarily, connects machines. Authors have also described the evolution of the Internet in stages. First, the Internet served as a point-to-point communications tool for human users. Later, the development of the World Wide Web (Internet 1.0) transformed the Internet into a system for organizing and retrieving human-generated information. Internet 2.0 involved the appearance of platforms to enable human business and social transactions. The IoT evolution moves the Internet beyond its anthropocentric roots to become a system for interacting with the broader physical environment. Fully realized, IoT technology means that the ICT architecture will change the way we gather information about the physical environment, and, for many parts of that environment, the way that we exercise control. Some of that control will continue to be exercised by humans, and some likely will not (see discussion in Section 3.2, *Analytics, Cognition and Autonomy*).

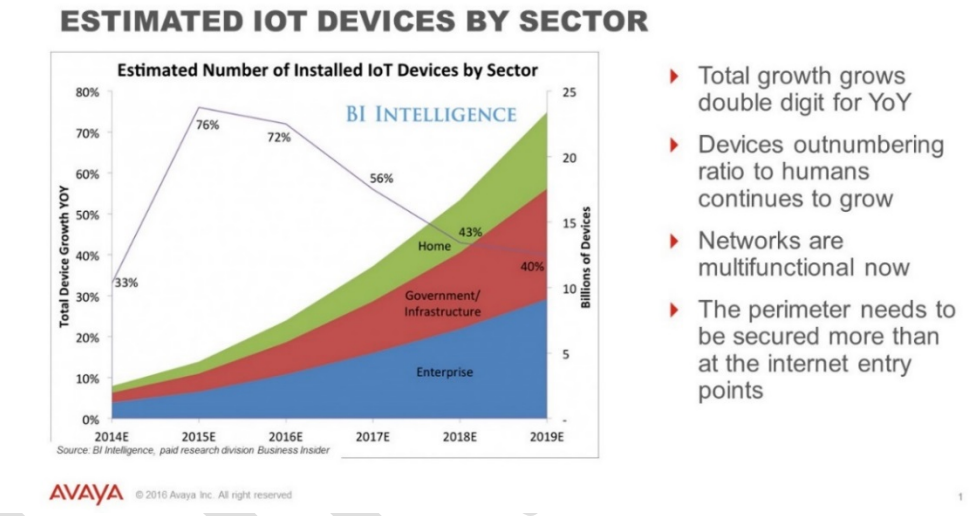

Figure 3.6. Estimated IoT Devices by Sector to 2019[31]

The cybersecurity implications of IoT derive principally from the vast multiplication of potential attack surfaces, along with inadequate or immature security practices when developing and deploying IoT devices. As demonstrated in the recent Mirai botnet attacks,[32] some already-deployed IoT devices lack basic security features that could prevent them from being hijacked for use in a DDoS attack. This is partially a legacy problem, as many IoT devices were manufactured and installed without the security precautions that would be routine for the installation of a regular network device like a router or server. The people who installed and configured the devices may not have considered them as full-fledged network components that would benefit from features such as upgradability and encryption. However, there are also more persistent issues. For example, many already-deployed IoT devices, and certainly many devices

[31] BI Intelligence, paid research division Business Insider. Paul Unbehagen. Avaya Networking. *Briefing to the NSTAC ETSV Subcommittee.* October 4, 2016.

[32] Lily Hay Newman. "The Botnet that Broke the Internet Isn't Going Away." December 9, 2016, https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

in the current supply chain, may lack an accessible interface that allows the user to configure passwords, authentication settings, and other security settings. In addition, incentives to invest in security may be insufficient, especially for non-traditional technology providers or startups.

For this first generation of IoT cybersecurity challenges, key actions will be to create a proper security culture around IoT devices by providing small and large enterprises with the expertise and incentives to remove non-configurable devices from supply chains and utilize secure design practices to ensure deployed IoT devices are properly configured. Over a longer timeframe, trends in IoT present additional cybersecurity challenges that organizations will need to meet with a more strategic response, such as integrating secure development practices into popular Integrated Development Environments.

Sensors in the fully realized IoT will be extremely numerous and very small, potentially presenting unique challenges. Briefers described sensors that could be embedded in paints or road coating, woven into fabrics, sprayed on surfaces, etc. Ultimately, sensors could exist as near-nano technology that is surgically implanted, injected, or ingested by animals and humans. (See Section 3.3, *Production and Simulation*, for a discussion of forthcoming developments in materials science and nanotechnology.) However, the small size of IoT sensors, and resulting constraints on computing power, communications bandwidth, and storage capacity, will limit the functions that can be accommodated. As a result, security features like encryption and authentication might be crowded out, and some sensors might not be physically or remotely upgradable.

Furthermore, IoT exists within an ecosystem that adds complexity to existing cybersecurity challenges. Individual sensors may be generic devices that use available networks to connect to application software that, in turn, presents or delivers information to an end user (whether human or an automated control system). Responsibility for securing the ecosystem will likely be distributed between and among the device manufacturer, the application provider, the network provider, and the end user.

The situation described above would likely benefit from very well-coordinated security standards and a studied, holistic approach to any regulation. This has not typically been the approach taken by the Government, however, and the rapid pace of current IoT deployment increases the likelihood of haphazard, reactive regulation. Moreover, since the ICT infrastructure is global, a coordinated approach will need to encompass not only U.S. Government actions but also the actions of many other countries' governments as well as international organizations.

NS/EP Impacts:

IoT will create a data-rich environment that could substantially improve the Government's situational awareness in the event of a significant incident. If properly managed, IoT information could give responders a much better picture of a population's locations and movements. IoT-controlled infrastructures could also aid in impact assessments, first responder resource allocations, and evacuations. However, to realize these capabilities, Government NS/EP components must have the ability to interact with the available IoT infrastructure and to process

IoT-generated data. In this respect, IoT mirrors many of the issues the NSTAC examined in its 2016 study of big data analytics.[33]

NS/EP planners may also need to adjust the prioritization of emergency communications. For example, if current plans prioritize the re-establishment of voice (wired and wireless) communications, then future plans may need to take more account of the broadband data infrastructure that supports IoT. Similarly, NS/EP planners may need to start treating parts of the IoT architecture as critical infrastructure that should be protected during incidents. For instance, if at some point in the future a substantial portion of the health care delivery system incorporates IoT solutions, then medical sensors and their associated devices will need protection and should be prioritized over less sensitive IoT devices. Fully leveraging IoT solutions in emergency situations will require NS/EP authorities to grapple with cross-cutting issues related to interoperability, user accessibility, individual privacy, cybersecurity, message authentication, and users' reactions to emergency messaging.[34]

Finally, cybersecurity challenges have already emerged as a major concern in the IoT context. As noted above, a great deal of uncertainty exists concerning how security and authentication responsibilities should be allocated in the complex IoT ecosystem. For example, since many IoT devices are small and possess limited onboard resource space, some manufacturers have shipped devices without security features that are common in larger connected devices. As IoT enters the Government's own ICT infrastructure, the Government must ensure that proper security and data protection measures are in place. This is particularly true for critical NS/EP systems that may start to leverage IoT devices.

Key Concepts	NS/EP Benefits	NS/EP Risks
Smart devices – ranging from consumer products to industrial infrastructure – produce, use, and process information to improve how they function or related services	• More data generation to inform analytics, cognition, and autonomy – aiding in impact assessment, first responder resource allocation, evacuation, etc	• Challenges related to data protection, data integrity, and maintaining cross-border data flows • Scale of attack surface (e.g., botnets)

[33] NSTAC. *NSTAC Report to the President on Big Data Analytics*. May 11, 2016. https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Big%20Data%20Analytics%20%284-22-16%29%20%282%29.pdf.

[34] Jon Eisenberg. National Academies of Sciences, Engineering, and Medicine. *Briefing to the NSTAC ETSV Subcommittee*. July 19, 2016.

3.1.3: 5G (Near-Term Transformative)

Introduction:

The arrival of the 5G wireless platform will markedly improve the capacity and latency of existing cellular networks. Moreover, 5G is expected to make robust and high quality broadband data available in large quantities and at relatively low costs. The promise of 5G is essentially to complete the evolution of wireless technology from a voice-centric technology to a data-centric one. Some briefers also indicated that 5G could eventually enable wireless to supplant the wired architecture for the delivery of broadband services. In this way, 5G could expand the existing footprint of network dense areas.

What is 5G?

5G refers to the next (fifth) generation of wireless technology. The specific features of 5G are not yet formally defined, but it will likely use high frequencies (millimeter wave) on the cellular spectrum and be delivered through smaller and more numerous antenna sites. 5G is expected to have a much higher capacity and much lower latency than existing 4G networks.

Discussion:

Designated 5G, the next generation wireless protocol is expected to have codified standards and widespread deployment by 2020. While not yet fully defined, 5G will typically involve larger numbers of small cell sites than what is used with existing networks, and it will feature both higher capacity and lower latency than 4G networks. As a result, 5G will enable the deployment of many of the other technologies discussed in this report, including IoT, autonomous vehicles, and advanced VR and AR. Additionally, 5G's low latency will enable incredibly precise remote control, with numerous applications that are beyond the scope of this report (i.e., telemedicine, drone operations, and remote robotic assembly).[35]

5G technology also builds from SDN/NFV developments. In particular, 5G technology and architecture will involve disaggregation of the radio access network (RAN) and the centralization and virtualization of the RAN control infrastructure.[36] As mobile packet core functions become virtual functions in the NFV infrastructure, there may be dramatic optimizations in how mobile traffic gets routed; for instance, more distributed and SDN-enabled traffic routing may reduce round-trip latencies. This disaggregation and virtualization also offers an opportunity to diversify and distribute the mobile infrastructure. However, similar to the security implications of SDN and NFV discussed above, it also increases the importance of securing RAN locations and the virtualized control infrastructure.

[35] Robert Cheng. "Not Just Speed: 7 Incredible Things You Can Do With 5G." March 2, 2017. https://www.cnet.com/news/5g-not-just-speed-fifth-generation-wireless-tech-lets-you-do-vr-self-driving-cars-drones-remote/.

[36] Kin-Yip Liu. "Splitting, Slicing, and Disaggregating the RAN towards 5G." February 28, 2017. https://www.wirelessweek.com/article/2017/02/splitting-slicing-and-disaggregating-ran-towards-5g.

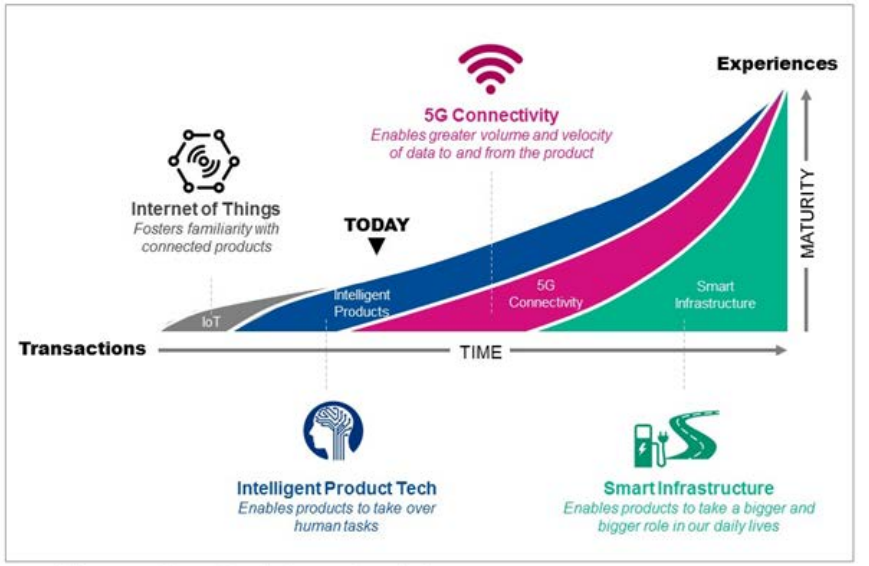

Figure 3.7. IoT and 5G Will Converge to Support a Smarter and More Data Intensive Physical Infrastructure[37]

Several briefers noted the criticality of 5G as an enabler of IoT and other technologies, stressing the need for Government action to enable rapid deployment of a 5G infrastructure.[38] Such action could deal with spectrum availability issues, harmonize regulatory approaches, and address infrastructure siting issues at the State and local levels. Briefers also pointed out that the security of the 5G infrastructure should receive great priority, and that the shift to 5G represents another opportunity to get cybersecurity right. In particular, shifts in trust models (i.e., as whole industries and unattended machines and sensors connect) and service delivery models (i.e., as telecom operators host third party applications in their clouds) should be considered.[39]

NS/EP Impacts:

5G provides an opportunity to use the agility of virtualization deployments to improve NS/EP response in providing and recovering communications. In addition, as s an enabling technology, 5G's NS/EP impacts are more indirect than those of the emerging technologies that it will support (e.g., IoT, smart infrastructures, VR, autonomous vehicles). The arrival of 5G in the relatively short term (i.e., within two to three years) will likely accelerate the deployments of these other technologies and will put pressure on the Government to address their NS/EP impacts. As a potentially ubiquitous network, 5G may raise trust and authentication issues as the number and scope of devices attempting to connect to networks increase.

While IoT and other 5G-supported emerging technologies promise a broad range of social and economic benefits, the NSTAC notes that these benefits will not be delivered equally. IoT will

[37] Gary Barnabo and Alexandra Heckler. Booz Allen Hamilton, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* August 16, 2016.

[38] Please refer to Section 5.0, *Recommendations,* for more information.

[39] Ericsson. *5G Security.* June 2015. https://www.ericsson.com/assets/local/narratives/industries/public-safety/wp-5g-security.pdf.

first be realized in environments of high network density and among early adopters of higher capacity wireless infrastructure. The availability of sufficient spectrum, as well as other infrastructure, to enable such networks is an important priority for industry and will need to be supported by Government policy at the Federal, State, and local levels.[40] Outside of network-dense environments, the benefits of IoT and other technologies may be significantly limited or substantially delayed. To the extent that NS/EP planning begins to incorporate the IoT infrastructure, the Government will need to address this potential disparity in access to 5G.

Key Concepts	NS/EP Benefits	NS/EP Risks
Much higher capacity and much lower latency networks will enable other emerging technologies to proliferate and mature	• Other emerging technologies will likely depend on 5G to operate/advance, including IoT, VR/AR, and autonomous vehicles	• As a wide range of devices and services, with different security requirements and levels of criticality, will be supported by 5G, there may be challenges related to building new trust models for security and privacy

3.1.4: Wireless Mesh Networking (Near-Term Transformative)

Introduction:

Wireless mesh networking emerged more than one decade ago,[41] but its deployment is set to accelerate. As the rise of IoT increases demand for ubiquitous network access, it will likely drive growth in alternatives to cellular-based access (e.g., 5G), including both wireless mesh networks and solutions that build upon the existing infrastructure of Wi-Fi access points. Mesh techniques offer a simplified way to scale and support more devices over a wide area quickly, creating new wireless networks or extending existing wireless local area networks.

A wireless mesh network is an ad hoc network that, once established, wirelessly connects devices directly to each other without needing to pass through a central authority or server.

What is a wireless mesh network?

Mesh networks can leverage various types of radio signals and allow different types of devices, each acting as nodes, to build on each other and create a wider, more robust network. Each device, or network node, spreads the signal a little further than the last, and each node interacts with others to amplify the signal. Thus, unlike a traditional WiFi network where a device communicates with a single access point and signal is impacted by distance and location, wireless mesh networks may better scale with demand as IoT devices themselves act as network nodes. In fact, IoT devices may be configured to interconnect across disparate systems, enabling dynamic network connections between and across many nodes.

[40] Please see Section 5.0, *Recommendations,* for more information.

[41] Matthew Broersma. "Mesh Network: The Next Step for Wireless." April 5, 2004. http://www.zdnet.com/article/mesh-networking-the-next-step-for-wireless/.

While wireless mesh networks are often perceived as a valuable tool in the context of emergency response, they may also provide regular means for communication.[42] For instance, in a connected home scenario, devices associated with the heating, ventilating, and air conditioning system may connect with household appliances, the home's security system, or other sensors on the property. These connections could essentially form an ad hoc network that could be configured so that newly added devices join this web/mesh of connections, rather than directly accessing the home's central Wi-Fi network.

Discussion:

As highlighted in Section 3.1.2, *Internet of Things (Near-Term Transformative)*, the potential positive impacts of IoT are many, but connectivity is integral to supporting IoT devices, enabling the use of big data, and building machine learning and AI capabilities. 5G and an increased number of Wi-Fi access points will support greater connectivity, but wireless mesh networking may also be deployed to meet demands for ubiquitous network access. Moreover, software-defined wireless mesh networks may offer improvements to network visibility and management.[43]

Wireless mesh networking may also be a particularly appropriate technology to support connectivity in certain contexts, fulfilling the need for networks in areas in which there is limited network infrastructure. Wireless mesh networks have been used to support connectivity in the aftermath of disasters, when standard communications infrastructure has been damaged or overloaded. For example, in the aftermath of Hurricane Sandy in 2012, mesh kit router nodes linked with mobile devices (which can be used as additional nodes that extend a wireless mesh network) enabled residents of the largest residential complex in Brooklyn to have Internet access, even though power, cell service, and Wi-Fi access in their homes was limited or not yet re-established.[44] Over the wireless mesh network, residents were then able to use social media to alert people to their needs or to check on relatives.[45]

This capability may also be useful to support connections among IoT devices that, like mobile devices, may act as network nodes, especially in areas with less robust broadband access. One IoT use case for this capability is connected cars or, as further discussed below, autonomous vehicles. As shown in Figure 3.8, using wireless mesh networking, vehicles could form a mesh that enables chained communications. This would allow vehicles to bypass the limitations of their short-range transmitters, such as distance or line of sight.

[42] Primavera De Filippi, "It's Time to Take Mesh Networks Seriously (And Not Just for the Reasons You Think." January 2, 2015. https://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/.

[43] Prithviraj Patin, Akram Hakiri, Yogesh Barve, and Aniruddha Gokhale, "Enabling Software-Defined Networking for Wireless Mesh Networks in Smart Environments." IEEE. 2016. http://www.dre.vanderbilt.edu/~gokhale/WWW/papers/NCA16_SDN_WMN.pdf.

[44] Becky Kazansky. "In Red Hook, Mesh Networks Connects Sandy Survivors Still Without Power." November 12, 2012. http://techpresident.com/news/23127/red-hook-mesh-network-connects-sandy-survivors-still-without-power.

[45] Ibid.

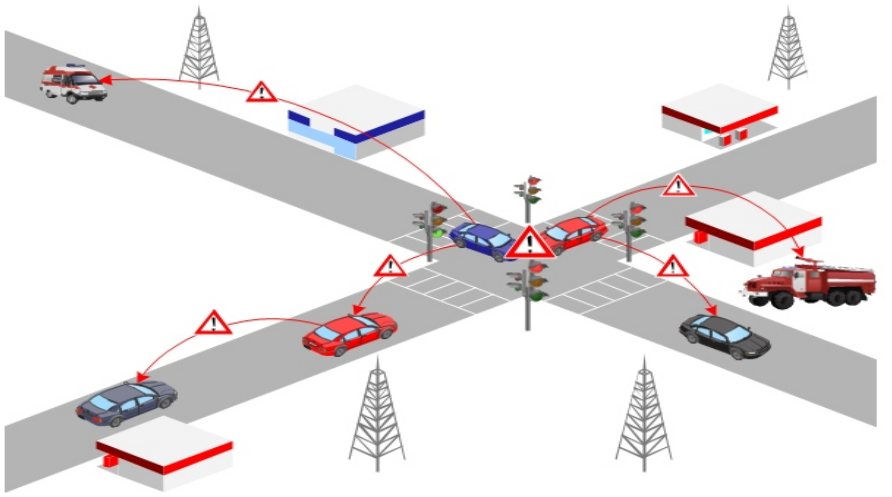

Figure 3.8. Mesh Networking and Vehicle Communication[46]

Another context in which wireless mesh networks may be particularly useful is in promoting resiliency and redundancy. While the use cases for such resiliency are potentially wide-ranging, one clear benefit is having wireless mesh networks in place to ensure connectivity in the aftermath of disasters (i.e., when traditional network infrastructure is damaged) or during crises (i.e., when simultaneous user demand overloads traditional networks). Wireless mesh networks can also automatically reconfigure themselves based on the availability and proximity of bandwidth and storage. In recent years, consumer-friendly mesh networking kits and apps, including Serval, Commotion, and FireChat,[47,48] have become increasingly available, making the technology more accessible to everyday users.

As shown in Figure 3.9, wireless mesh networking can be used to supplement traditional cellular communications by enabling the exchange of information between nearby devices. To support resiliency, small mesh networks, such as those existing within a single home, could be connected with nearby homes to create a much larger mesh. The process could be repeated again and again, leveraging different aspects of the IoT infrastructure. Mesh networks could also leverage smart cities devices, connected cars, and a host of other distributed nodes. Additionally, it would be possible to configure cellphone handsets, which already contain radio transmission hardware, as small network access points. Theoretically, these practices could create a dense, readily available network in parallel to the traditional wireless and wired infrastructure.

[46] Vehicular Ad-Hoc Network. "Security and Privacy in Location-based MANETs/VANETs." Accessed on April 10, 2017. http://www.ics.uci.edu/~keldefra/manet.htm.

[47] Tom Simonite. "Build Your Own Internet with Mobiles Mesh Networking." July 9, 2013. https://www.technologyreview.com/s/516571/build-your-own-internet-with-mobile-mesh-networking/.

[48] Alan Yu. "How One App Might Be a Step Toward Internet Everywhere." April 7, 2014. http://www.npr.org/sections/alltechconsidered/2014/04/07/298925565/how-one-app-might-be-a-step-toward-internet-everywhere.

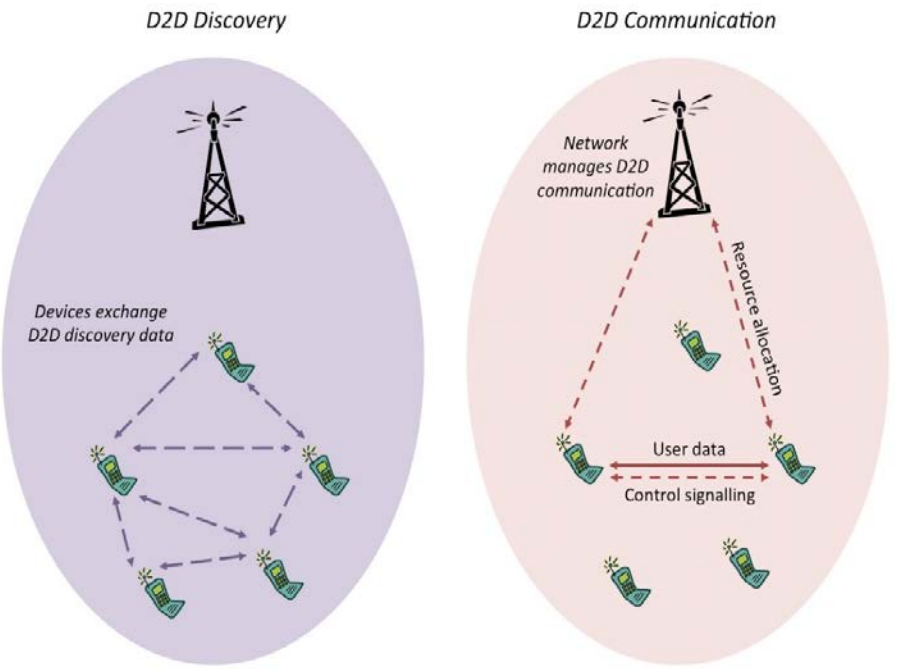

Figure 3.9. Mesh Networking and Cellular Communications[49]

NS/EP Impacts:

The NS/EP implications for wireless mesh networks are intriguing. Such networks offer the promise of increased resiliency and provide an alternative to existing communications infrastructures. As a widely distributed network infrastructure, mesh networks may prove more survivable than fixed infrastructures in some situations. Like SDN, mesh networks also offer the possibility of creating ad hoc networks in the aftermath of an event, potentially accelerating the recovery of communications and improving the situational awareness of first responders.[50] However, while these approaches are promising, they will still encounter some limits, as even meshed and virtual networks rely on some physical infrastructure. But advanced planning and widespread access to consumer-friendly mesh networking apps will support broader use.

On the other hand, mesh networks, like IoT, may also create new security challenges. The promiscuous connectivity that is at the heart of mesh networking is counter to cybersecurity best practices. In addition, controller security of mesh networks managed by SDN or SDN-like controllers is critically important. Therefore, substantial work on the security of mesh networks that is focused on authentication, encryption, and other communications security measures may need to be done before the NS/EP benefits of the technology can be fully realized.

[49] Alaister Brydon. "Opportunities and Threats from LTE Device-to-Device (D2D) Communication." February 28, 2014. http://www.unwiredinsight.com/2014/lte-d2d.

[50] Jay Turner. "Responding to Disaster With IoT and SDN mesh." December 23, 2016. https://techcrunch.com/2016/12/23/responding-to-disaster-with-iot-and-sdn-mesh/.

Key Concepts	NS/EP Benefits	NS/EP Risks
Ad hoc networks that, once established, wirelessly connect devices to each other without needing to pass through a central authority or server	• Can be built in the aftermath of an event, increasing response capabilities • Provide an alternative to existing communications infrastructures and increase survivability due to widely distributed infrastructure, increasing resilience	• Widespread connectivity counter to existing cybersecurity best practices • Work on authentication, encryption, and other security measures is necessary

3.1.5: Quantum Computing (Long-Term Transformative)

Introduction:

Quantum computers represent a revolutionary development that will alter the foundations of computer science and bring an almost unimaginable increase in computing power. While quantum technology is complex and could be realized in many different forms, there is widespread agreement that quantum computing will become a reality within 10-20 years. Quantum computers will affect many disciplines, but it is their theoretical ability to defeat existing encryption protocols that is most immediately concerning from an NS/EP perspective.

The topic of quantum computing and its potentially transformational effects are of great interest and concern to the NSTAC. While some briefers described quantum computing as one of numerous forms of future computing architectures with extraordinary, revolutionary potential (including biocomputing and neuromorphic computing[51,52]), this section focuses on quantum developments and impacts, which is consistent with most briefers' overwhelming focus on quantum computing. As in so many discussions surrounding quantum computing, the NSTAC encountered a variety of opinions regarding exactly when a meaningful version of this technology will arrive, but there was no disagreement as to the certainty of its eventual existence.

Classical computers encode information in bits that can take the value of 1 or 0; these 1s and 0s act as on/off switches that ultimately drive computer functions. Quantum computers, on the other hand, are based on qubits, which operate according to two key principles of quantum physics: superposition and entanglement. Superposition means that each qubit can represent both a 1 and a 0 at the same time. Entanglement means that qubits in a superposition can be correlated with each other; that is, the state of one (whether it is a 1 or a 0) can depend on the state of another. Using these two principles, qubits can act as more sophisticated switches, enabling quantum computers to function in ways that allow them to solve problems that are intractable using today's computers.

What is quantum computing? [53]

[51] Computational Paradigms. Accessed on: April 14, 2017. https://aqpl.mc2.chalmers.se/~chaparall/ComputationalParadigms.html#Neuromorphic.

[52] Roundtable, Department of Energy, Office of Science. "Neuromorphic Computing: From Materials to Systems Architecture." October 29-30, 2015. https://science.energy.gov/~/media/bes/pdf/reports/2016/NCFMtSA_rpt.pdf.

[53] IBM. "What is Quantum Computing?" Accessed on: June 21, 2017. http://research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

The NSTAC was briefed about some of the currently operating quantum machines and on efforts to develop compilers, operating systems, and applications for future quantum computers. The NSTAC received information on the current state of quantum research, both in the United States and in other countries, though briefers were limited to unclassified information, given the public nature of the NSTAC's work.

Discussion:

The theories supporting the operation of a true quantum computer are extraordinarily complex and well beyond the scope of this report. In the simplest terms, traditional computers operate in a binary state—all information is ultimately expressed as "1" or "0" for processing in the computer's physical architecture. A quantum computer would escape the binary limitation; it would be capable of holding information as simultaneously "1" and "0" and in other states between "1" and "0" as well. With regard to these changes, some briefers noted that computer scientists currently lack even a consistent vocabulary to explain quantum operations. Fully realized quantum computing will bring about a foundational transformation in computer science and many related disciplines.

The term quantum computing encompasses a variety of technical approaches to achieving quantum operations, some of which are highlighted in Figure 3.10. In other words, quantum is not a unitary project; there are many distinct approaches and models currently being pursued. Each approach yields different capabilities, and there are many complex relationships and technical interdependencies at work in this field.

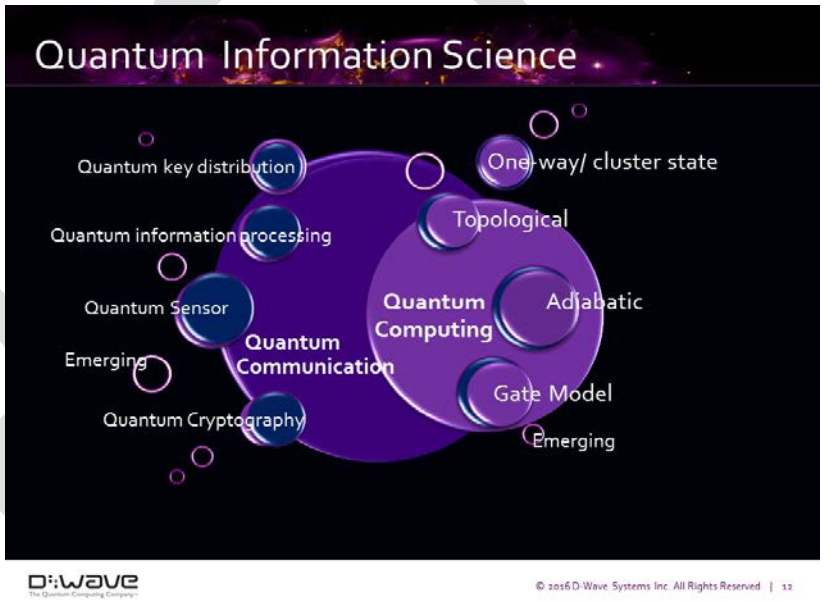

Figure 3.10. Quantum Information Science[54]

Some of these approaches have already yielded quantum machines, though these machines are limited to very specific operations or to a brief period of functioning in a testbed environment. For example, the NSTAC was briefed by one company that operates machines that are capable of quantum annealing, which is a specific function that leverages quantum properties and that may be useful in certain applications. These briefers explained that a full quantum computer is a much more complex undertaking and depends on a number of yet-to-be accomplished developments that are essential to the stability of a true quantum computer. Figure 3.11 illustrates some of the necessary steps towards more robust quantum technology.

[54] Robert Ewald. D-Wave International. *Briefing to the NSTAC ETSV Subcommittee.* November 1, 2016.

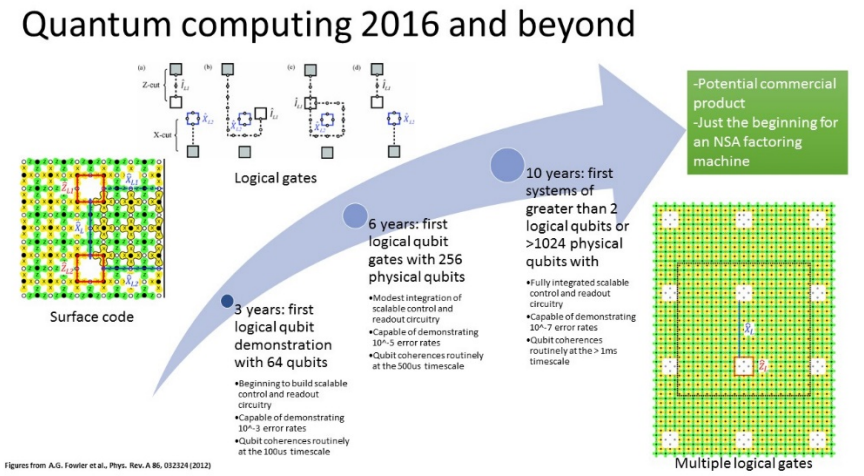

Figure 3.11. Quantum Computing in 2016 and Beyond[55]

Fundamentally, across various approaches to quantum technology, the arrival of sufficiently stable and powerful quantum computing represents a revolutionary shift in processing power.[56] Because they are not limited by binary data values (i.e., 0, 1), quantum objects can represent significantly more data; in addition, quantum algorithms, which are specifically designed to harness the computational power of quantum objects, perform computations much faster than any classical computing algorithm.[57] This profound amplification of processing power could have many important applications, driving progress across diverse fields. For instance, quantum computers could support complex research simulations, which are less precise today because of the limitations of traditional computing.[58] In addition, vast increases in processing power could rapidly advance efforts to improve machine intelligence.[59]

In the national security environment, however, quantum computing and the impact of such an expansion in processing power tend to refer to the development of a cryptologically meaningful quantum computer, which would be sufficiently developed to manipulate cryptological algorithms. In particular, a quantum computer will be cryptologically meaningful when it is stable and developed enough to leverage quantum processing power in support of Shor's algorithm, a quantum algorithm for integer factorization (in simple terms, it can find the prime factors of any integer).[60] Such a quantum computer, relying on its immense processing power and the special characteristics of quantum mechanics, could theoretically break nearly all public key encryption currently in widespread use.

---

[55] Dr. Thomas Ohki. Raytheon BBN Technologies. *Briefing to the NSTAC ETSV Subcommittee.* November 8, 2016.

[56] NIST. "Quantum Computers May Have Higher 'Speed Limits' Than Thought." March 24, 2017. https://www.nist.gov/news-events/news/2017/03/quantum-computers-may-have-higher-speed-limits-thought.

[57] Brad Jones. "Quantum Computing Will Make You Look Like a Graphing Calculator." September 19, 2016. http://www.digitaltrends.com/features/dt10-quantum-computing-will-make-your-pc-look-like-a-graphing-calculator/.

[58] Philip Ball. "Quantum Computer Simulates Hydrogen Molecule." July 25, 2016. https://www.chemistryworld.com/news/quantum-computer-simulates-hydrogen-molecule/1010041.article.

[59] Peter Diamandis. "Massive Disruption Is Coming With Quantum Computing." October 10, 2016. https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/.

[60] The mathematics of the algorithm are very complex. In 2007, another mathematician produced a "non-technical" explanation that Peter Shor later identified as "the best explanation of quantum computing for the man in the street" that he had seen. Scott Aaronson. "Shor, I'll Do It." February 24, 2007. http://www.scottaaronson.com/blog/?p=208.

NSTAC briefers suggested that even a very basic version of such a quantum computer is probably at least 10 years away and depends on many intervening developments. However, the deployment of quantum-resistant public key encryption will also take significant time to deploy. Put another way, in the arms race between computing power and encryption, there is not yet a decisive winner emerging—though there are significant potential risks at play as well as opportunities to advance more substantially in progress on quantum-resistant encryption (as further discussed below in Section 3.4, *Trust and Verification*).

NS/EP Impacts:

The national security implications of quantum computing are easy to discern, as the first nation state that develops a cryptologically meaningful quantum computer will obtain an enormous strategic advantage over its adversaries. The nation state would not only be able to decrypt intercepted adversary communications (that are not protected by quantum-resistant encryption) but also reap an intelligence windfall through the decryption of archived, but still encrypted, intercepts. The implications of these developments are not limited to the Government context. Quantum decryption capabilities will threaten all encrypted data and will undermine the security of financial and other business systems as well as personal communications.[61]

The race for quantum computing is, in some respects, unlike previous research and development (R&D) efforts. Often, speakers invoke comparisons to the Manhattan Project or the Apollo program when discussing quantum computing. While it is undeniable that large, Government-centered R&D programs should occur for quantum computing, the Government should not lose sight of the surrounding environment. The promise of quantum computing is not just applicable to military or crypto systems. The transformative effect of quantum extends to communications, big data, financial analysis, and a host of other commercial functions. To the extent that these functions also enable the Government's NS/EP efforts, there will be second order effects.

The broad applicability of quantum also means that quantum projects have already attracted very significant capital investment in the private sector, both in the United States and abroad. Unlike the development of nuclear weapons during the Manhattan Project, quantum computing has been researched and discussed openly in academic environments for almost 25 years. A well-funded private sector effort therefore is not necessarily at a disadvantage to a classified Government program. Indeed, an NSTAC briefer noted that the talent pool for high-end work on quantum projects is quite small and internationally distributed. Private sector efforts may actually have an advantage over the Government in this area, as the private sector can attract talent by offering positions free from the onerous security requirements of classified Government work.

The NSTAC recommends that the Government review its own R&D efforts towards quantum systems and consider how to defend against the possibility that another state actor—or a private sector actor—obtains such capabilities before the United States does.[62] The Government should consider what its national security strategy might be if the first quantum power was a U.S.

[61] It should be a strategic priority for the Government to ensure that the United States is the first to obtain these quantum computing capabilities, and an overview of ongoing research efforts may be in order. The NSTAC is indirectly aware that significant U.S. research efforts are underway in classified environments, but the NSTAC was not briefed on these efforts and is not in a position to evaluate them. However, the NSTAC has been briefed on the broader efforts taking place in the private sector and on what is known openly about efforts in other countries.

[62] Please see Section 5.0, *Recommendations*, for more information.

company, a foreign company, or a multinational company with uncertain ties to any one jurisdiction. While it is still too early to predict how close we are to the end of the race toward meaningful quantum, the Government should adopt a broad enough strategic vision to ensure that it is not caught unaware by the arrival (and ownership) of this technology. The estimates the NSTAC heard ranged from 10-20 years, though all briefers noted that any number of breakthroughs in computational or material science could substantially accelerate that timeline.

Finally, the Government should consider whether the United States possesses the ability to control the pace of progress towards quantum through restrictions on strategic components. One commonality in present-day quantum computing projects is the requirement for extreme refrigeration technology. Quantum operations require temperatures approaching absolute zero (0 Kelvin). For example, the quantum annealing machines described to the NSTAC operated at .0015 Kelvin. The technology used to achieve these temperatures is based on the use of certain helium isotopes. The United States is the world's major supplier of helium, and briefers noted that most current research efforts, including those supported by foreign governments, likely utilize helium-based refrigeration technology from U.S. suppliers. Given this, if it has not already begun to do so, the NSTAC would recommend that the Government consider whether export restrictions on key refrigerants and related technology might be warranted.

Key Concepts	NS/EP Benefits	NS/EP Risks
Through superposition and entanglement, qubits can act as sophisticated switches, enabling quantum computers to solve new and more difficult problems	• Ability to decrypt communications and data protected by public key encryption • Leap forward in computation power, enabling analysis of more data in parallel and more complex modeling, simulations, and AI	• Inability to safeguard communications and data not protected by quantum-resistant encryption

3.1.6: Summary: Interconnectivity and Processing Power Impacts

The forthcoming explosive growth in interconnectivity and processing power will be driven both by the rapid deployment of already maturing technologies and by the arrival of transformative developments that essentially re-write the basic rules of computing. The NSTAC foresees the decline of static infrastructure in favor of flexible, distributed, and virtual ICT architecture; an environment of ubiquitous sensors leveraging ubiquitous connectivity that yields nearly unimaginable amounts of data; networks that are reconfigured to manage this shift; and human communications being dwarfed by rapidly expanding machine-to-machine communications. Just over the horizon are radically different computing technologies that will vastly expand processing power and significantly disrupt legacy operations.

These developments will have significant implications for NS/EP operations. Rapid deployment may outstrip considered and well-coordinated security measures. NS/EP situational awareness may be improved by ubiquitous sensors and greater data granularity, but they also may be degraded by non-static architectures. The challenge for the Government will be to leverage the promise of the new technology while managing ever-evolving security threats.

3.2 Analytics, Cognition, and Autonomy

The technologies discussed within this section have captured imaginations for decades, in manifestations ranging from Isaac Asimov's *Robot* series to the *Terminator* and beyond—and recent technology advancements are enabling significant progress. In particular, new classes of inexpensive sensors, cloud computing, increasingly cheap and incredibly fast parallel computation,[63] and more powerful algorithms have provided the big data as well as the storage and processing capabilities necessary to teach AI, unlock new possibilities for neural networks, and generate the 60-years-in-the-making overnight success of AI.[64]

There are many different functions and a range of maturity levels in technologies often commonly referred to as AI, bots, or robots, and NSTAC briefers and other sources have different ways of characterizing forthcoming developments. For example, some differentiate between narrow and general AI, explaining that narrow AI allows an application to perform a very specific function, whereas general AI consists of capabilities that more closely resemble the full range of human intelligence and self-improving capabilities. Others refer to weak and strong AI, with the latter being sentient and/or sapient. Because there are many ways to disambiguate between the various technologies, capabilities, and levels of maturity that are often considered as within an AI ecosystem, before considering the various technologies and capabilities that are on the horizon, this section first introduces the taxonomy used here:

- Machine learning – fundamental AI capabilities that are associated with various approaches to analytics or other processes for assessing data and reasoning;
- Near-term AI – early AI with specific functionality, typically focused on a narrow task;
- Natural language processing – AI capability that involves not just translating but also automatically parsing and understanding unstructured and structured text and spoken language, within and across multiple human and machine languages;
- Long-term AI – mature AI with a specialized but high functioning capability or with a range of capabilities, potentially including or going beyond a full range of human intelligence capabilities; and
- Semi to fully autonomous units, devices, or systems – entities that use AI to collect, assess, and/or share data; make decisions; and/or act with or without human intervention.

Technologies discussed within this analytics, cognition, and autonomy trend include:

- Near-term AI (e.g., security bots);
- Natural language processing;

[63] Advancements in parallel processing are due to developments in chip technologies, especially graphics processing unit and field programmable gate arrays.

[64] Kevin Kelly. *The Inevitable: Understanding The 12 Technology Forces That Will Shape Our Future* (2016), page 40.

- Long-term AI; and
- Autonomous vehicles (i.e., land and air).

Figure 3.12 highlights these technologies as they were represented above in Figure 2.2.

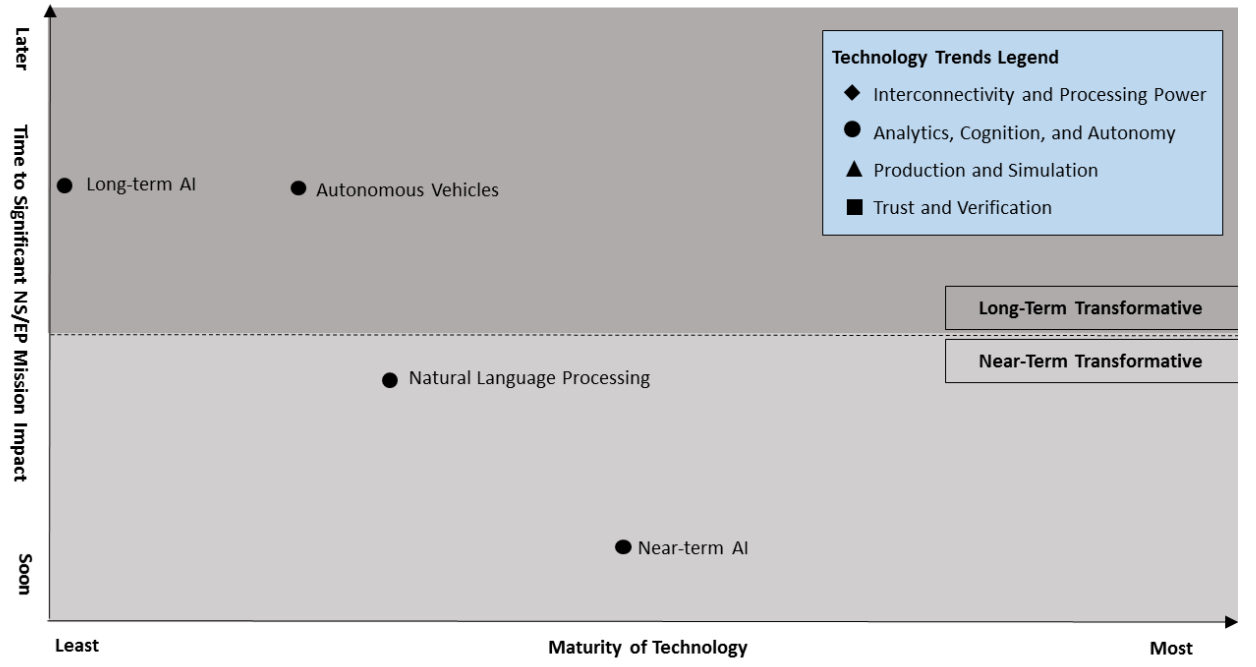

Figure 3.12. Analytics, Cognition, and Autonomy

3.2.1: Near-Term AI (Near-Term Transformative)

Introduction:

Near-term AI encompasses a broad range of technologies and capabilities with which many people are familiar or commonly interact, including personal assistants like Alexa, Cortana, and Siri; search engine queries; targeted advertising; language translation services; photo tagging; and recommendations engines that suggest movies or other products that consumers may enjoy. Near-term AI is also being applied to more complex problems, such as diagnosing medical conditions or beating advanced opponents in difficult games. IBM's Watson famously did so on the quiz show Jeopardy! in 2011, and AI again made the news in 2016 when a Deep Mind computing system beat a top human player at the ancient board game Go, a "contest of strategy and intuition that has bedeviled AI experts for decades."[65]

Near-term AI is early AI with specific functionality, such as the ability to play a game, make a medical diagnosis, drive a car, defend a network, or assess the impact of a natural disaster. Across domains, such functionality is powered by big data and machine learning algorithms that enable AI to assess information and make appropriate predictions, learning and improving over time.

What is near-term AI?

[65] Cady Metz. "In A Huge Breakthrough, Google's AI Beats a Top Player at the Game of Go." January 27, 2016. https://www.wired.com/2016/01/in-a-huge-breakthrough-googles-ai-beats-a-top-player-at-the-game-of-go/.

While the Go victory was suggestive of increasing AI creativity, in January 2017, an AI program developed by Carnegie Mellon researchers went even further, showing that it could bluff when it crushed top poker players at Texas Hold 'Em.[66]

There are at least two core functions of near-term AI: assessment and prediction. Assessment involves using big data and machine learning to develop characterizations, rules, or other forms of understanding through analytically-based reasoning, reasoning from evidence, or deep learning. Prediction will be further discussed below.

- Analytically-based reasoning involves the translation of pattern recognition into mathematical equations or rules.[67]

- Reasoning from evidence involves pulling together various pieces of information, each with varying degrees of value, to arrive at a potential answer.[68]

- Deep learning involves methods of pre-cognitive reasoning, (i.e., teaching computers "from the ground up" [from data] rather than "from the top down" [from rules]).[69]

Deep learning is currently thought of as the cutting-edge of the cutting-edge in machine learning, in part because, through enormous data inputs and advanced algorithms, it enables computer systems to use data to make decisions about other data—meaning it cuts across and can complement other approaches to assessment and prediction.[70] Data is processed through neural networks, or logical constructions that ask binary questions, extract values, and classify data—and as these networks develop, they become deep neural networks with significant logic complexity that are sophisticated enough to handle extremely large data sets, such as Twitter's firehose of tweets.[71] Moreover, these systems train themselves based on new data inputs and can learn from mistakes. As such, deep learning is foundational to the navigation of self-driving cars, predicting the outcome of legal proceedings, precision medicine (tailored to an individual's

---

[66] Maureen Dowd. "Elon Musk's Billion-Dollar Crusade to Stop the AI Apocalypse." March 26, 2017. http://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x.

[67] For example: if A = 1, then B = 1; if A = 2, then B = 2; if A = 3, then B = ? We know that B = 3 because of the relationship between the data points. In a data set presented to AI, the relationship would be much more complex, and there would often be gaps in information and uncertainties, but the approach would remain the same: start with data; then look for trends, correlations, and other mathematical relationships that inform assessments.

[68] For example, data points may include: a person was a man, a person was a German, a person was a refugee, a person was a famous scientist – and the answer may be: who was Albert Einstein? In this way, all indicators are accrued into a final piece of reasoning, and there may be a score or a degree of likelihood for a potential answer, which may be one among many potential answers. This approach not only informed the reasoning used by Watson on Jeopardy!, but also informs the reasoning used by AI programs that support medical diagnostics.

[69] Gideon Lewis-Krauss. "The Great AI Awakening." December 14, 2016. https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html?_r=2. For example, deep learning is similar to the recognition techniques that humans use when we look at a "chair" and know it's a chair. The data inputs may be machine signals, written words, video, speech/audio signals, a set of pixels on a screen, all of the sensor inputs from a self-driving car—and reasoning will determine, through knowing many features in association with different objects or outcomes: it is a known song, it is a particular position on a Go board, or it is a pedestrian.

[70] Bernard Marr. "What is the Difference Between Deep Learning, Machine Learning and AI?" December 18, 2016. https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#4517ab7026cf.

[71] Ibid.

genome), automated analysis and reporting, and playing games such as Go.[72] Deep neural networks have also enabled recent advancements in image recognition, speech recognition (which reached human parity in late 2016), and language translation—though, as discussed below, language understanding is an even more complex endeavor. [73,74]

Deep learning and the other above-described approaches to machine learning help to achieve a core function of near-term AI: assessment. In addition, those functions can be combined with time, collaborative filtering, and/or other contextual information to develop predictions or recommendations. Predictive analytics start with analytically-based reasoning, reasoning from evidence, or deep learning and add time stamps, shifting the question from one situated as a snapshot in time to one that can extend over a future period of time. Recommendation analytics start with those core functions and information about a known entity and set of behaviors (e.g., a consumer's past transactions), as well as other known entities and their sets of behaviors (e.g., other consumers' past transactions). Through collaborative filtering of behaviors, recommendations can be made. For instance, if two consumers have made similar choices but one has made more choices (e.g., X bought A, B, and C and Y bought A, B, C, and D), then an additional choice may also resonate with the similarly behaving consumer as a recommendation (e.g., X may also want to buy D).

Discussion:

Algorithms that enable the core functions that are foundational to near-term AI have many potential applications. In short, in any situation or context, more intelligence—whether in the form of analytically-based reasoning, reasoning from evidence, or deep learning—could enable more preparedness, more informed decision making, more precision, and/or more consistency on a faster time scale and with less room for human error. As the EOP National Science and Technology Council (NSTC) Committee on Technology wrote in October 2016, AI has already positively impacted health care, transportation, the environment, criminal justice, and economic inclusion—as well as the effectiveness and efficiency of the Government itself.[75]

Near-term AI may also be applied to advance cybersecurity, especially if human and machine intelligence can be combined in a way that optimizes efficiency. Today, both humans and machines play key roles in security, with the former focusing on the analysis of known rules and the latter focusing on anomaly detection, often resulting in false positives that must be assessed and corrected by humans. In the context of finding more complex and unexpected threats, machines lag behind humans, and finding data needed to drive machine learning in the security world is difficult. However, numerous public and private sector organizations are investing in

[72] Ibid.

[73] Allison Linn. "Historic Achievement: Microsoft Researchers Reach Human Parity in Conversational Speech Recognition." October 18, 2016. https://blogs.microsoft.com/next/2016/10/18/historic-achievement-microsoft-researchers-reach-human-parity-conversational-speech-recognition/#sm.0000t2h5i97yof7sqc02rp17ws9iz.

[74] Gideon Lewis-Krauss. "The Great AI Awakening." December 14, 2016. https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html?_r=2.

[75] Executive Office of the President National Science and Technology Council Committee on Technology. *Preparing for the Future of Artificial Intelligence*. October 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

driving progress. Last year, for example, researchers from the Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory and the machine-learning startup PatternEx demonstrated that a platform called AI2 predicts cyber attacks much more effectively than existing systems by continuously incorporating input from human experts.[76] In addition, in 2016, the Defense Advanced Research Projects Agency's Cyber Grand Challenge pitted seven autonomous security bots against each other, working to patch holes in their own machines while exploiting holes in the others.

In responding to some cybersecurity threats, such as major DDoS attacks, approaches that leverage truly autonomous, self-improving security bots may also be impactful, as positive emergent behavior (i.e., the development of larger systems from smaller, autonomous units) can counter negative emergent behavior. Specifically, in the future, autonomous responses by larger defender systems (positive emergent behavior) to attacks like the Mirai botnet (negative emergent behavior) could look like this:

- Smart routers collect their own data, do an on-board analysis, and share their data and analysis within a decentralized trust network (e.g., supported by blockchain); and

- Smart routers collectively identify malicious patterns, identify that global optima may override local instructions, and deny traffic en masse.

In essence, such a decentralized, automated incident response would function like an organic Security Operations Center (SOC) rather than the current, classic response in which individual SOCs identify anomalous traffic patterns and intervene manually.

However, near-term AI must further develop to enable such applications. Such approaches may be enabled by further progress on semi-autonomous technologies[77] and experiments that tackle the challenges of autonomy.[78] In addition, to achieve effective autonomous, self-managing systems, investment in several emergent technologies and related research areas is needed:

- Autonomous communications channels[79] for big data;

---

[76] Specifically, the researchers showed that AI2 can detect 85 percent of attacks, which is about three times better than previous benchmarks, while also reducing false positives by a factor of five. Creating systems that merge human- and computer-based approaches is difficult, in part because manually labeling cybersecurity data for the algorithms is challenging—and the process of reviewing reams of suspicious data is time-intensive for busy experts. However, AI2 "fuses together three different unsupervised-learning methods," showing the top events to experts and building a supervised model that it can constantly refine. Adam Conner-Simons. "System predicts 85 percent of cyber attacks using input from human experts." April 18, 2016. http://www.csail.mit.edu/System_predicts_85_percent_of_cyber_attacks_using_input_from_human_experts%20.

[77] One NSTAC briefer highlighted that semi-autonomous security technology that mirrors and responds to risky behaviors—and is capable of learning/adapting environments without human supervision—is fundamental to maturing near-term AI.

[78] One NSTAC briefer described the challenges of autonomous cyber defense as including an expanding attack space; growing potential for unpredictable behaviors; greater likelihood for intentional abuse; and increasingly decentralized data/response.

[79] One NSTAC briefer noted that continued accumulation of big data is necessary but not sufficient; in addition, each big data system will need its own autonomous communications channel, rather than command and control, allowing proactive response.

- Pervasive semantic technologies capable of utilizing self-regulating ontologies and taxonomies (more capable of learning from their environment);

- Deep learning algorithms that can complete complex inferences under conditions of uncertainty;

- AI that can form appropriate value judgments and not just fulfill logic (i.e. evaluate costs, benefits, and consequences);

- Blockchain, which will provide distributed trust amongst autonomous machines; and

- The mathematics of emergent behavior (econometrics, computer science, computational linguistics/biology).[80]

While there are enormous potential benefits to near-term AI in the security context and much more broadly, there are also risks inherent in near-term AI functions and processes. In particular, large-scale machine learning can be rendered ineffective if the data or algorithms upon which it is based is low quality or biased in some way. For instance, "most common" does not necessarily equate with "most true," and if our data sets or algorithms are biased, then machines will inherit and potentially even accelerate bias.[81] Moreover, if we become overly dependent on machine learning or fail to be transparent about data sets and/or algorithmic processes, then we may also lose the ability to see that bias.

As a result of such concerns, in addition to education and research programs that focus on building out the technology and mathematics to support future applications of AI, education and research programs that focus on maintaining and growing understanding of algorithms and machine-to-machine communication should be a critical priority.[82] Relatedly, an area of focus in ongoing R&D efforts is the need to maintain algorithmic transparency, establish guidelines for algorithms, and secure algorithms to ensure that they are not manipulated.

As R&D proceeds and AI impacts new domains and markets, there may also be efforts to capture progress in global technology standards forums. To prepare for developments related to emerging technologies such as near-term AI, the Government should increase its investments in such standards forums. While industry-led, consensus-based efforts to develop standards to support transparency and interoperability will be critical, global technology standards forums with government participants will likely also undertake efforts to standardize aspects of emerging and enabling technologies. As other governments have expanded their participation and investments in such standards forums, and in some cases currently dominate relevant forums, it is critical that the U.S. Government also commit to a long-term investment in those forums to support U.S. innovation and competitiveness as well as a more secure ecosystem.[83]

[80] Please refer to Section 5, *Recommendations*, for more information.

[81] Anthony Scriffignano. Dun and Bradstreet Corporation. *Briefing to the NSTAC ETSV Subcommittee.* October 18, 2016.

[82] Please refer to Section 5, *Recommendations*, for more information.

[83] Ibid.

For instance, once standardized, approaches that support algorithmic security or transparency may more easily spread throughout the ecosystem and be embedded in AI going forward.

NS/EP Impacts:

Just as near-term AI can positively impact many situations and contexts, so too can it positively impact the Government's NS/EP mission. In particular, in the context of emergencies, there is often a general need to process and analyze vast amounts of data quickly to direct efforts most efficiently. Numerous services have started to leverage near-term AI for such purposes. For instance, Artificial Intelligence for Disaster Response has developed algorithms to automatically identify relevant tweets during disasters; similarly, Digital Jedis use AI to identify relevant features in pictures, satellite imagery, and aerial imagery.[84] More broadly, One Concern uses AI both to prepare for emergency scenarios through realistic scenarios and to respond in the wake of a disaster, quickly obtaining situational awareness that enables responders to direct resource allocation and identify evacuation routes.[85] As part of this process, One Concern uses seismic data and structural knowledge of buildings to judge which parts of a city will be most at risk in an earthquake and to prioritize rescue efforts.[86]

As near-term AI becomes increasingly distributed, however, there will likely also be NS/EP challenges. First, in an emergency or crisis, individuals or organizations may receive conflicting guidance from AI applications and designated officials; for example, individuals using mobile map applications may go in a particular direction—one that's being blocked by officials attempting to route traffic the other way. Second, as introduced above, there is a significant risk of using biased data or algorithms to inform near-term AI. When there is little time to review AI decision making, there may be risk in relying on AI for various tasks, such as the identification of victims or perpetrators of attacks. Third, there is a risk of AI algorithm security. If AI algorithms can be manipulated in a cyber attack, then there may be risk in officials or the broader population relying on them during a crisis or emergency.

Key Concepts	NS/EP Benefits	NS/EP Risks
Early AI with specific functionality powered by big data and machine learning algorithms	• The ability to utilize advanced planning capabilities • The ability to analyze vast amounts of data quickly to direct efforts most efficiently • More precision and more consistency on a faster time scale	• Lack of algorithmic transparency and accelerated human bias • Security challenges (e.g., manipulation of algorithms) • Dependency on apps; lack of coordination with officials

[84] Patrick Meyer. "Digital humanitarians, big data and disaster response." February 19, 2015. https://www.brookings.edu/blog/techtank/2015/02/19/digital-humanitarians-big-data-and-disaster-response/.

[85] One Concern. Accessed on April 14, 2017. http://www.oneconcern.com/

[86] Chris Baraniuk. "Earthquake Artificial Intelligence Knows Where Damage Is Worst." September 30, 2015. https://www.newscientist.com/article/mg22830412-800-earthquake-artificial-intelligence-knows-where-damage-is-worst/.

3.2.2: Natural Language Processing (Near-Term Transformative)

Introduction:

Natural language processing, or semantic disambiguation, poses unique challenges to near-term AI. Each of the above-described, near-term AI core functions and approaches to machine learning have seen tremendous advancements in the last three-to-five years, in part because of the incredible amounts of data that are being generated and applied to help AI learn; however, progress in the context of national language processing has been slower.

> Natural language processing is the process of automatically parsing, analyzing, and understanding structured and unstructured text and spoken language across multiple languages.

What is natural language processing?

While data has been foundational for progress in translating between languages, it has been less powerful in addressing the broader issues of natural language processing, including bridging the gap between how language is used and what it means. Because of the intricate nature of language, this is incredibly challenging; colloquialisms, grammar and punctuation, varying dialects, sarcasm, and other unique linguistic oddities all disrupt AI understanding. Figure 3.13 highlights some of the complexities of natural language processing, including determining the intended meaning of common terms or names, understanding who is speaking to whom and what impact that may have, and shifting smoothly through other contextual variations.

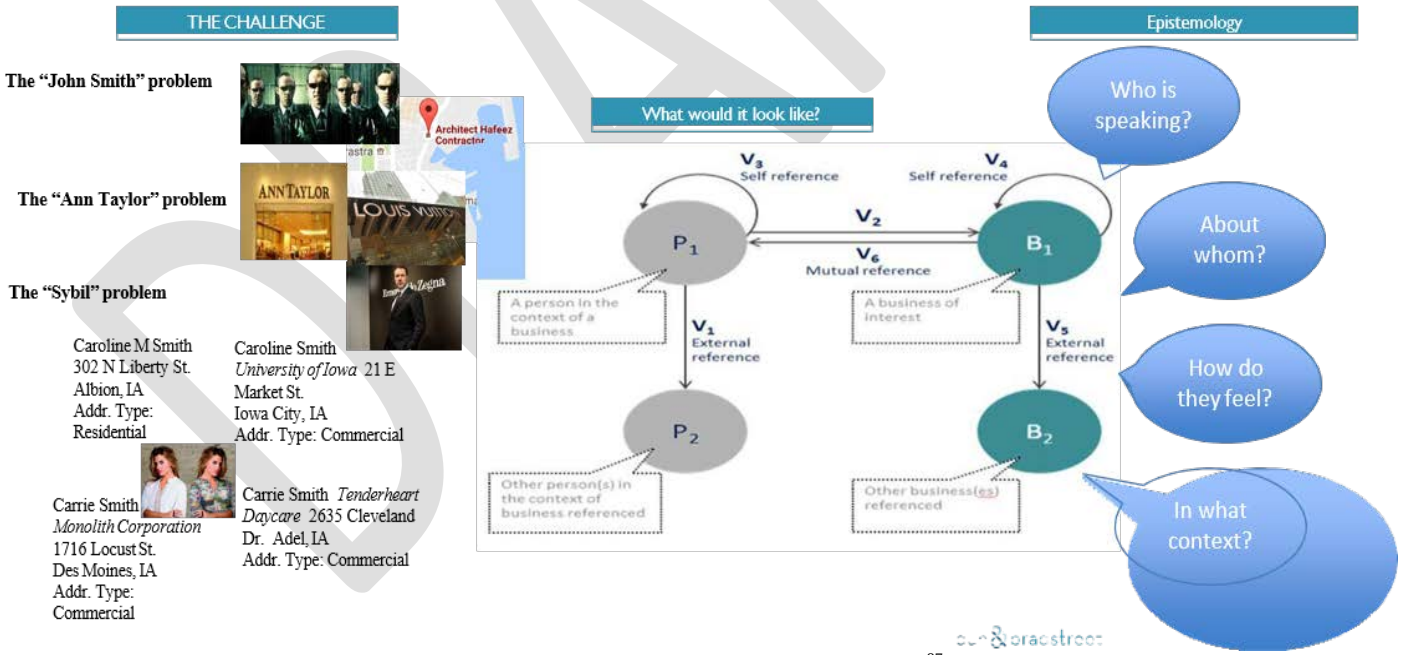

Figure 3.13. Complexities of Natural Language Processing[87]

[87] Anthony Scriffignano. Dun and Bradstreet Corporation. *Briefing to the NSTAC ETSV Subcommittee.* October 18, 2016.

Discussion:

Natural language processing has many potential applications, including distinguishing conversations of interest from other noise, detecting relationships between entities of interest and their behaviors, and bridging gaps in human-AI interactions.[88] Though malicious actors try to use sophisticated cloaking techniques in digital communications to avoid detection, natural language processing has already been used to detect malicious activity, including money laundering, corporate identity theft, and illicit trade rings. In addition, one limitation of certain forms of near-term AI may be human hesitation to trust machine learning and reasoning, especially since AI's ability to communicate meaningfully with humans may be constrained in certain contexts. For example, in medical diagnostics, while AI is able to score its potential answers (e.g., 74 percent certain), humans may often seek a better understanding of how an answer was obtained. To the extent that natural language processing can help bridge that gap by translating machine communication, it may also open up new possibilities for the use of near- and long-term AI. Moreover, in the future, natural language processing may be able to accomplish more nuanced activities, such as the translation of machine-to-machine communication, enabling machines that use different formats and structures to communicate and humans to understand communications among and decision making by coordinating machines.

NS/EP Impacts:

In the NS/EP context, advanced natural language processing may act as an enabler for greater use of emerging technologies as it helps to bridge gaps in human-human, human-AI, and machine-to-machine communication. In crises or emergency situations, such capabilities may quickly increase transparency and trust in first responder communications, AI algorithms, and autonomous machine activities, including positive emergent behavior. In addition, in national security situations, natural language processing may be used to quickly increase situational awareness through the nuanced interpretation of communications between and among potential perpetrators of an attack. However, natural language processing may also be vulnerable to the near-term AI risks and challenges described above.

Key Concepts	NS/EP Benefits	NS/EP Risks
The process of automatically parsing, analyzing, and understanding structured and unstructured text and spoken language across multiple human and machine languages	• Bridging gaps in human-human, human-AI, and machine-to-machine communications • Distinguishing conversations of interest and detecting relationships between entities of interest	• Lack of algorithmic transparency and accelerated human bias • Security challenges, (e.g. manipulation of algorithms)

[88] Ibid.

3.2.3: Long-Term AI (Long-Term Transformative)

Introduction:

AI is currently a form of symbiotic intelligence based on algorithms derived from human experience.[89] As AI continues to learn, AI algorithms and capabilities continue to advance, and our vocabulary for AI continues to evolve, the range of possibilities for AI will also expand. Ultimately, the context in which long-term AI is deployed will further define its requirements and expected functions, which will likely evolve and expand over time.

Long-term AI is mature AI with specialized but very high functioning cognitive capability or with a range of cognitive capabilities, potentially including or going beyond a full range of human intelligence capabilities.

What is long-term AI?

Discussion:

While ideas about what long-term AI will look like abound, they might all manifest to some degree, and some may transcend others.

- AI may consist of a general set of capabilities, closely resembling the full range of human intelligence capabilities, like a highly advanced version of SoftBank's/IBM's Pepper robot. Pepper uses deep learning to operate with a range of functions as diverse as taking orders at some U.S. Pizza Hut locations to providing financial advising services in Japan. When SoftBank first released Pepper in 2015, before further powering it with IBM's Watson, SoftBank touted it as the world's first device that can read human emotions. As of May 2016, close to 10,000 Peppers were sold worldwide.

- AI may do narrow tasks with extreme intelligence and efficiency. Rather than a Pepper-like machine (with human-like consciousness), such AI would look like an advanced version of hyperscale cloud services—cheap, reliable, and industrial-grade digital smartness running behind everything.[90] Rather than being impacted by messy self-awareness, such AI will be akin to a set of special purpose software brains that we trust to do specific tasks, such as driving a car or translating from any language to any other language, but little else.[91]

- AI may be highly and uniquely personal and/or contextual, providing the right information at the right time in the right format for the right person.[92] In this case, the next big thing would not necessarily be a thing (e.g., a robotic personal assistant), but rather a change in relationships among technologies, among people, and between humans and technology. The complexity between devices is growing beyond the threshold of frustration, and humans can only handle a certain amount of complexity, after which they may eschew devices altogether. AI could help us avoid that threshold, enabling responsibilities to shift seamlessly from device to device and managing complete

[89] Ibid.
[90] Kevin Kelly. *The Inevitable: Understanding The 12 Technology Forces That Will Shape Our Future* (2016), page 33.
[91] Ibid, page 42.
[92] William Buxton, Dr. Jie Liu, and Dr. Evelyn Viegas. *Briefing to the NSTAC ETSV Subcommittee.* July 26, 2016.

continuity of operations (e.g., continuing a call made through the onboard computer in an automobile with a mobile device when exiting the vehicle, without degradation of service or capability). This also correlates with the idea of the graceful augmentation and degradation of functionality in devices (e.g., adding the capability to make hands-free calls or removing the capability to play mobile games while driving)—context dependent, but also fluid and natural functionalities. In addition, while today's technologies often force people to devote their full attention to a device rather than their surroundings, combining technologies could make devices seem less conspicuous for users. For example, outdoor advertisements in public spaces may display targeted or unique cues, visible to users through smart glasses, to provide directions instead of requiring users to pull out and monitor a mobile phone. Another manifestation of this approach may be augmenting human capabilities to enable broad accessibility, even in contexts in which disabilities have previously limited it. For example, intelligent systems of auditory cues could be used to provide directions to the blind in a way that is as unobtrusive as headphones. Within industry today, there has been progress in leveraging a range of technologies to compensate for blindness, including visual recognition, advanced machine learning, and the creation of applications that run on a small computer that can be worn like a pair of sunglasses. This technology disambiguates and interprets data in real time, moving towards painting a picture of the world audibly instead of visually.

NS/EP Impacts:

Like near-term AI, long-term AI can positively impact many situations and contexts, including the Government's NS/EP mission. Humanoid robots with a full range of human intelligence capabilities, hyperscale smartness that can be integrated into everything, and highly personal and contextual intelligence could all support Government efforts to prepare for and respond to emergency situations. In addition, as above, if such cognitive capabilities are manipulated or plagued by bias, then there may also be challenges with using long-term AI in NS/EP contexts.

Beyond the NS/EP impacts that are foreseeable for near-term AI, long-term AI may introduce additional, more abstract NS/EP impacts. For instance, how long-term AI evolves may result in profound economic shifts. As investigated by the EOP last year, both near- and long-term AI may necessitate occupational shifts, as some skills may be more cheaply and reliably performed by AI than humans.[93] Driving is a common example, as the short-term unemployment that may result from replacing human truck and taxi drivers with AI truck and taxi drivers could be significant. However, if long-term AI tends more towards "nerdily narrow, super smart specialists,"[94] then AI may augment human professionals, rather than replace them. In *The Inevitable: Understanding The 12 Technology Forces That Will Shape Our Future*, Kevin Kelly writes that, today, the best chess player is a centaur—a human/AI cyborg—and computer chess games have helped humans play more often and be better than ever at chess. Similarly, AI can help humans become better pilots, better doctors, better judges, and better teachers.[95] In the context of NS/EP, AI can help humans become better first responders, such as better Emergency

[93] Executive Office of the President. *Artificial Intelligence, Automation and the Economy.* December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf.

[94] Kevin Kelly. *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (2016).

[95] Ibid, pages 41-42.

Medical Technicians. Likewise, if long-term AI tends to focus on changing relationships among and between humans and technology, then the augmentation of humans may enable more people to take on a broader range of jobs.

While it may be challenging to predict exactly how AI will evolve and "which jobs will be most immediately affected by AI-driven automation,"[96] education, training, and re-training programs that help prepare the human workforce for forthcoming AI-driven shifts, not only in employment opportunities but also in the nature of many jobs, are critically important.[97] Such education, training, and re-training programs, coupled with other policy initiatives, will be important to enable the United States to not only manage short-term workforce challenges but also prepare to take advantage of the next waves of innovation, which will likely create new workforce opportunities in the NS/EP space and drive global economic competition. As Alec Ross wrote in *The Industries of the Future*, greater societal comfort with the integration of robotics in economies like Japan and China may mean that they leap ahead in the application of such devices and technologies.[98] Likewise, the U.S. Department of Defense (DOD) and other AI developers within the Government are sensitive to the U.S. public's perception of the technology, impacting approaches to integrating and using AI.[99] As described above in the section on cloud computing and SDN/NFV,[100] being an early adopter and user of technology has significant dividends, including the ability to shape the evolution of the technology and to be prepared to leverage future technologies that build on top of it.

In addition, there are significant governance questions regarding the rise of nearly or even fully conscious, broadly intelligent AI systems, and the Government should partner with industry in evaluating them, building from the efforts undertaken by the NSTC last year.[101] According to most experts, the risk is not a humanoid robot; it is the intelligent, self-improving algorithm.[102] There are ongoing private sector efforts to address AI opportunities and challenges,[103] including algorithm transparency, which was also highlighted in the NSTC's report.[104] The Government should be a partner, contributing to the dialogue and research and raising public awareness of ongoing efforts to develop AI in a way that has broad societal benefits. There are also related

---

[96] Executive Office of the President. *Artificial Intelligence, Automation and the Economy.* December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf.

[97] Ibid. The future is not necessarily bleak; previous generations of increased automation, which eliminated all but one percent of previously dominant agricultural jobs, also created hundreds of millions of jobs in new fields. Likewise, AI will result in new opportunities that accrue significant economic benefits, but like previous shifts precipitated by technological progress, those benefits "will not necessarily be evenly distributed across society." The more that both the U.S. Government workforce and the Nation's broader workforce are prepared to find new opportunities and to use AI to enhance how they accomplish their work, the less stressful forthcoming, AI-driven shifts will be, both to individuals and to the U.S. and global economy. Please refer to Section 5, *Recommendations*, for more information.

[98] Alec Ross. *The Industries of the Future* (2016).

[99] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.

[100] Please refer to Section 3.1, *Interconnectivity and Processing Power*, for more information.

[101] EOP: NSTC. *Preparing for the Future of Artificial Intelligence.* October 2016.

[102] Maureen Dowd. "Elon Musk's Billion-Dollar Crusade to Stop the AI Apocalypse." March 26, 2017. http://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x.

[103] Partnership on AI. Accessed on: April 4, 2017. https://www.partnershiponai.org/#.

[104] EOP: NSTC. *Preparing for the Future of Artificial Intelligence.* October 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

safety and regulatory challenges that must be addressed; one near-term manifestation of this challenge is ensuring the safe roll out of autonomous vehicles, which are further discussed below, as well as highlighted in the NSTC report.[105] The Government should also clarify contexts in which full autonomy is acceptable and examine liability and other legal issues in cases in which there may be costs, or other negative impacts, due to the use of AI in autonomous devices, units, or systems. In doing so, as highlighted in the NSTC report, there should be a focus on ensuring that regulatory responses do not overly burden the development of such forthcoming innovation.[106]

Key Concepts	NS/EP Benefits	NS/EP Risks
Mature AI with specialized but very high functioning cognitive capability or with a range of cognitive capabilities, potential including or going beyond a full range of human intelligence capabilities	• Range of assistance from intelligent, autonomous units during emergencies, potentially including human-like capabilities, specialist support, and/or context-specific support • Advancements in preparing, planning, integrating experiences and lessons learned	• Lack of algorithmic transparency and accelerated human bias • Security challenges, e.g. manipulation of algorithms • Major economic shifts and governance issues, including NS/EP workforce and regulatory challenges

3.2.4: Autonomous Vehicles (Long-Term Transformative)

As with AI generally, there are numerous manifestations of robots or entities that use AI, including devices, self-driving cars, drones, and more popularized conceptions of bi-pedal robots that might complete a variety of tasks, including assist in emergency contexts.[107, 108, 109] In addition, such entities may be embedded with and use varying degrees of autonomy, taking direction from humans, interacting with humans, or making decisions independent of human involvement. This section discusses semi-to-fully autonomous land and air vehicles, focusing on two potential manifestations of this forthcoming AI/robotic technology rather than covering the range of bi-pedal robots and other devices that will likely be embedded with AI in the future.

Autonomous vehicles are entities that use AI to collect, assess, and share data; make decisions; and act (i.e., move) without human intervention.

What are autonomous vehicles?

[105] Ibid.
[106] Ibid.
[107] While a thorough discussion of the variety of bi-pedal robots that may emerge is beyond the scope of this study and report, there is significant ongoing research on the development of such robots and applications in the NS/EP context. In addition, those robots will benefit from deep neural networks and advances in image recognition technology, enabling them to operate in unknown environments. World Federation of Engineering Organizations. Accessed on: April 4, 2017. http://www.wfeo.org/next-generation-technology-disaster-preparedness-relief/.
[108] EKU Online. "When Disaster Strikes: Technology's Role in Disaster Aid Relief." Accessed on: April 4, 2017. http://safetymanagement.eku.edu/resources/infographics/when-disaster-strikes-technologys-role-in-disaster-aid-relief/.
[109] NIST. "Emergency Response Robots." September 21, 2016. https://www.nist.gov/programs-projects/emergency-response-robots.

Autonomous Land Vehicles

Introduction:

Autonomous land vehicles are somewhat old news on Mars (although a new model of Rover is being developed), but they are currently capturing the attention of auto manufacturers, consumers, and lawmakers back on Earth. Autonomous cars are poised to introduce and accelerate cascading changes, both in terms of their potential economic and NS/EP impacts and experientially as a future platform for connectivity, big data, and related services.

Discussion:

One potential future of autonomous cars looks like this:

1. An individual requests a car, and a nearby autonomous car responds for pick up;

2. The car arrives with optimal routing based on real-time traffic, traveling down smart roadways toward its destination and using its navigation system to communicate with other vehicles on the road, not only to avoid collisions but also to coordinate maximally efficient routing;

3. The car offers connected and personalized in-vehicle experiences, including screens that offer personalized shopping, VR experiences, interactions with friends and co-workers, and portable workspaces, and users expect that cars act as a platform through which they can access a larger range of personalized services, including health care sensors that identify if a user's blood sugar is low (for more on service platforms, see Section 3.3., *Production and Simulation*);

4. If the car witnesses any accidents or irregularities in route, it can automatically notify relevant emergency services;

5. The car will generate significant amounts of data about users, other vehicles, and the environment (each year, a car will generate more than six times the amount of data in the Library of Congress), all of which may be shared or sold, utilizing applications for anonymizing and sanitizing data before it is released, and bots will scan such exchanges for high-value data pertinent to an organization's interests;

6. The car may be re-charged by solar panels built into roadways or the car itself, enabling vehicles to wirelessly charge as they drive (the amount of solar energy that could be collected by the 31,000 square miles of U.S. highway has the potential to generate an energy supply three times greater than the country's current energy demand[110]); and

7. The car arrives at its destination and drops off the passenger, then determining whether it should drive itself to a nearby service, cleaning, or refueling station or park itself. (If the

[110] Rich Rogers. Hitachi, Limited. *Briefing to the NSTAC ETSV Subcommittee*. August 23, 2016.

car is semi-autonomous, then sensors will provide those managing vehicle fleets with visibility over all vehicle and user statuses, automatically notifying management of necessary maintenance or the need for emergency services.) Either way, with the operational context and environment in mind, predictive analytics will support just-in-time service and maintenance to maximize efficiency.

Technologies that are fundamental to this shift include IoT, which fosters consumer familiarity with connected products and service delivery; AI; and 5G connectivity, which is needed to provide the bandwidth necessary to quickly collect and use tremendous amounts of data. Within 20 years, autonomous vehicles will require greater bandwidth than homes.[111] In the meantime, a major challenge with deployment will be public concern about the safety of self-driving cars, particularly as accidents inevitably occur in the early stages of deployment.[112] As discussed above in the context of long-term AI, the Government should both engage the autonomous vehicle industry to minimize harms and normalize the industry with the public, evaluating ways to promote trust in this technology during its maturation and deployment cycles.

NS/EP Impacts:

The NS/EP impacts of autonomous land vehicles are wide-ranging. As the technology further develops, it may be increasingly useful to deploy autonomous vehicles to safely access disaster response areas. In addition, officials may utilize data from sensors in autonomous vehicles, generating real-time data to improve situational awareness, guide the public to greater safety, and determine how to deploy law enforcement and/or emergency responders—and their assets—in the most efficient and impactful way. Put another way, much like there is priority routing in wired and wireless communications systems in times of crisis, perhaps there should be automated priority routing for responders or autonomous emergency vehicles in times of crisis.

However, in addition to public perception and bandwidth challenges, such future applications of autonomous vehicles face NS/EP challenges, including privacy issues associated with public-private data exchanges. In addition, there are liability and security risks. Uncertainty exists around whether and when users, manufacturers, service providers, or others might be liable for autonomous vehicle accidents. There are also concerns about the cybersecurity of data sources and the amount of data being transported. Specifically, connected vehicles' physical and software components, as well as suppliers for those parts, have been recognized as potential attack vectors. Moreover, there are many entry points for attackers, including Bluetooth, Wi-Fi, vehicle-to-vehicle communication, charging stations, diagnostic tools, remotes, datacenters, and engines, as well as many risks related to data, services, and safety.[113]

In addition, consistent with the above section on long-term AI, multiple briefers stressed the need to develop AI algorithms that are secured against attacks—not just traditional availability attacks (which could degrade the efficiency of AI-dependent applications) but also attacks against the integrity of data. Simply put, if data integrity is compromised, then decision integrity may be compromised too.

---

[111] Gary Barnabo and Alexandra Heckler. Booz Allen Hamilton, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* August 16, 2016.

[112] Ibid.

[113] Ibid. There have been at least 16 major known vehicle hacks from March 2010-July 2016.

There have been significant auto industry responses to such risks, including:

- Original equipment manufacturers are implementing two sets of communications systems (to preserve and restore wireless connectivity and communications): one wireless- or 5G-based system, and a radio backup to ensure vehicle-to-vehicle and vehicle-to-individual communications if the primary system is rendered inoperable;
- Automakers have developed internal product cybersecurity initiatives;
- Automakers have formed the Auto Information Sharing and Analysis Center to promote collaboration among industry and between industry and Government;
- Automakers have developed a set of industry-wide best practices; and
- Automakers are integrating security into product design as part of their fundamental business model of promoting trust.[114]

In supporting R&D efforts to secure AI functions and applications against attacks in the context of autonomous vehicles, the Government should consider two areas of potential focus: (1) promoting resilient communications and autonomous operating systems to mitigate the threat to command and control centers; and (2) implementing integrity assurance measures for sensors and data streams, as well as the cross-correlation of sensor data, to help prevent the corruption of sensor data by AI applications.[115]

Key Concepts	NS/EP Benefits	NS/EP Risks
Entities that use AI to collect, assess, and share data; make decisions; and act (e.g., move on land) without human intervention	• Increased access in disaster response areas • Data from sensors in autonomous vehicles to increase situational awareness	• Privacy challenges with public-private data exchanges • Liability and security challenges • Risk of misuse by malicious actors (e.g., to cause accidents with other land vehicles or entities)

Unmanned (and Autonomous) Aerial Vehicles

Introduction:

Unmanned aerial vehicles (UAV) have captured national attention in the form of drones—both commercially available drones and those used in the context of national security. Some UAVs have varying degrees of autonomy and human control; trends suggest they will increasingly incorporate a growing degree of autonomy. The use of semi or fully autonomous UAVs in the national security context has raised questions relevant to NS/EP discussions about the degree to

[114] Gary Barnabo and Amanda Heckler. Booz Allen Hamilton. *Briefing to the NSTAC ETSV Subcommittee.* August 16, 2016.
[115] Please refer to Section 5, *Recommendations*, for more information.

which autonomy should be acceptable in the context of military operations,[116] but this section focuses on the use of semi or fully autonomous UAVs in the context of emergency response.

Discussion:

Emergency responders have repurposed three types of robots for disaster response: UAVs, unmanned ground vehicles, and unmanned maritime vehicles. However, UAVs are the most well-known and widely used. Due to their functionality and relatively low cost, UAVs are not only the most widely used form of robot in an emergency today but also predicted to become even more ubiquitous in all types of emergency response. Moreover, emergency responders typically have several data sources available after natural or man-made disasters: satellite imagery; manned helicopters; crowdsourcing and social media; and UAVs. While all are valuable, UAVs are especially so.[117] Quality UAVs that are small enough to fit in a backpack can be purchased for as little as $1,000 and often have video streaming capabilities. UAVs are also the fastest capability to deploy (whereas it usually takes the first search and rescue teams up to four hours to deploy)—and, in most natural disaster situations, while the availability of information increases over time, its impact and usefulness declines over time.

NS/EP Impacts:

UAVs serve multiple purposes, both before and in the immediate aftermath of an emergency, but their impact may be limited by technology constraints. Before an emergency, UAVs and the data they collect can be used to identify at-risk populations and assist with forensic predictions about how an event (e.g., a flood) will develop. In the immediate aftermath, ICT providers can use UAVs to deliver wireless communication capabilities to disaster-stricken areas. In addition, as a disaster unfolds, UAVs can be deployed to quickly collect data, enabling first responders to gather situational awareness and predict likely developments. Data collection and dissemination may present challenges, however. One 20-minute UAV flight can capture video and imagery of up to 30-40 acres; that means up to 800 high resolution images, requiring 1.7 gigabytes of data storage. With organizations often undertaking upwards of 200 UAV flights in response to a disaster, these UAVs collect more data than can be easily examined or distributed. In addition, data is often also collected in bursts, so large amounts of information suddenly becoming available can cause stress on data processing. Furthermore, these challenges are multiplied with more advanced capabilities; the memory-intensive nature of orthomosaics and VR renderings make them extremely difficult to transmit via email or to upload to cloud environments.

To manage and work around these challenges, emergency responders adopt different approaches. The team utilized by one NSTAC briefer conducts photogrammetry on localized desktop computers rather than in cloud environments and shares information via USB thumb drives rather than sending it over a network.[118] These tactics slow progress and waste time, which is particularly valuable in an emergency response context. Meanwhile, other organizations adopt tactics that may increase other risks. For instance, some non-governmental organizations have

[116] Future of Life Institute. "Autonomous Weapons: An Open Letter from AI & Robotics Researchers." July 28, 2015. https://futureoflife.org/open-letter-autonomous-weapons.

[117] Dr. Robin Murphy. Texas A&M University. *Briefing to the NSTAC ETSV Subcommittee.* August 30, 2016.

[118] Ibid.

posted high resolution images to a website and asked for the public's assistance in identifying signs of victims. In addition, because of their relative connectivity and functionality, in the context of numerous disasters, social media and messaging applications have been widely used, and AI applications[119] may also be increasingly used.[120] While there is clearly some value in crowdsourcing disaster response efforts and leveraging social media or other applications, there may also be privacy concerns with the disclosure of personally identifiable information. In addition, it is unclear to what extent application/content developers are connected with the Government and other parts of the communication infrastructure to plan and prepare for national emergencies appropriately.[121]

Multiple response organizations conducting their own UAV data collection efforts not only exacerbate the issue of tremendous amounts of data generation but also create additional challenges. Despite common operating mechanisms designed for information sharing, data is often inconsistently marked and shared. As a result, organizations are often either not aware of or unclear about how to use the data available to them. Data collected by UAVs and other robots may be more operationally impactful and more quickly used if information regarding its provenance was integrated into it, ensuring its integrity. Organizations like the Federal Emergency Management Agency have attempted to establish centralized data sharing hubs in response to individual disasters, including Hurricane Sandy, but organizations have not found them to be useful. The information shared has lacked proper provenance or context and has been restricted by authorization mechanisms that make it difficult for users to access. In addition, the computing storage requirements of central repositories are so extensive that few emergency response data centers exist that are capable of handling the collective sum of disaster information collected by stakeholders present on the scene of a disaster.

The following developments would help to address these challenges:

- The ability to handle fluctuating demands for resources and information;
- Visibility into the state of emergency response networks;
- The autonomous selection of alternative telecommunications systems;
- Context-sensitive prioritization and routing of data and communications;
- Cybersecurity mechanisms that allow new individuals from known organizations, as well as those from previously known organizations, faster access to centralized data sources; and
- Improved mechanisms for data provenance that protect integrity and enable confidence.[122]

[119] Mohana Ravindranath. "Alexa, Can You Tell Me About GSA's Virtual Assistant Pilot?" March 24, 2017. http://www.nextgov.com/emerging-tech/2017/03/alexa-can-you-tell-me-about-gsas-virtual-assistant-pilot/136457/?oref=site-nextgov-flyin-sailthru.

[120] World Federation of Engineering Organizations. "Engineering for Change." Accessed on: April 4, 2017. http://www.wfeo.org/next-generation-technology-disaster-preparedness-relief/.

[121] Please refer to Section 5, *Recommendations*, for more information.

[122] Dr. Robin Murphy. Texas A&M University. *Briefing to the NSTAC ETSV Subcommittee.* August 30, 2016.

From the NSTAC's perspective, increasingly intelligent and autonomous UAVs may also help to address some of these challenges. Across coordinating first responders, an interconnected network of UAVs could: (1) establish and maintain trust; (2) autonomously select and coordinate the use of telecommunications systems and routing decisions; and (3) make real-time decisions about what data is most relevant to collect/show as well as what degree of resolution is required. In addition, other forthcoming technologies, in particular 5G as well as wireless meshed networking, may help to increase bandwidth and connectivity options.

Key Concepts	NS/EP Benefits	NS/EP Risks
Entities that use AI to collect, assess, and share data; make decisions; and act (e.g., move in the air) without human intervention	• Increased visibility of disaster zones, pre- and post-disasters, at reduced operational costs • Delivery of communications capabilities	• Data privacy and integrity challenges • Risk of data interception and misuse by malicious actors (e.g., to attack physical infrastructures)

3.2.5: Summary: Analytics, Cognition, and Autonomy Impacts

Intelligence is already being integrated into a variety of different functions, including personal assistant applications, security bots, and autonomous vehicles. This trend is set to vastly expand in terms of dimension and impact, and experts suggest that the changes that it enables will ultimately be akin to that of electricity; in short, it will impact everything, including the Government's NS/EP functions and mission.

The Government is beginning to pay significant attention to AI. As discussed above, efforts by the EOP last year resulted in multiple reports on the future of AI and its impact on a range of public policy areas, including the workforce and strategic research priorities.[123],[124] In addition, the National Institute of Standards and Technology (NIST) Information Technology Lab (ITL) is shifting its attention to AI; in the last round of funding proposals received by NIST, the agency received more proposals related to machine learning and AI than anything else. ITL has since decided to establish a program building on its machine learning capabilities that could be used to propose funding projects in the future. In addition, NIST is beginning to consider the idea of securing AI, though it still lacks a comprehensive vision for what secure AI systems might look like. The NSTAC recommends that the Government continue to invest in AI algorithm and other related research to support and mitigate the risks of this forthcoming wave of technology.[125]

[123] EOP NSTC Council Committee on Technology. *Preparing for the Future of Artificial Intelligence.* October 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

[124] EOP. *Artificial Intelligence, Automation and the Economy.* December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf.

[125] Please refer to Section 5, *Recommendations*, for more information.

3.3 Production and Simulation

In recent years, many ICT vendors have moved from selling products to offering dynamic services and integrated platforms, which together create experiences. NSTAC briefers highlighted this shift in the context of autonomous vehicles (see also Section 3.2., *Analytics, Cognition, and Autonomy*). In this new world, an autonomous vehicle is not simply a device that moves people between locations; it is a platform that offers an array of services—including services that may prove important to first responders, such GPS, mapping, and data analytics. Dynamic services and integrated platforms mean lower costs and more agility in accessing products and services, in part because users can leverage services only when needed and in part because users can subscribe to only the service they will use. In addition, because they can be updated automatically over the air (rather than through shipped products), services enable more efficient iterations and improvements.

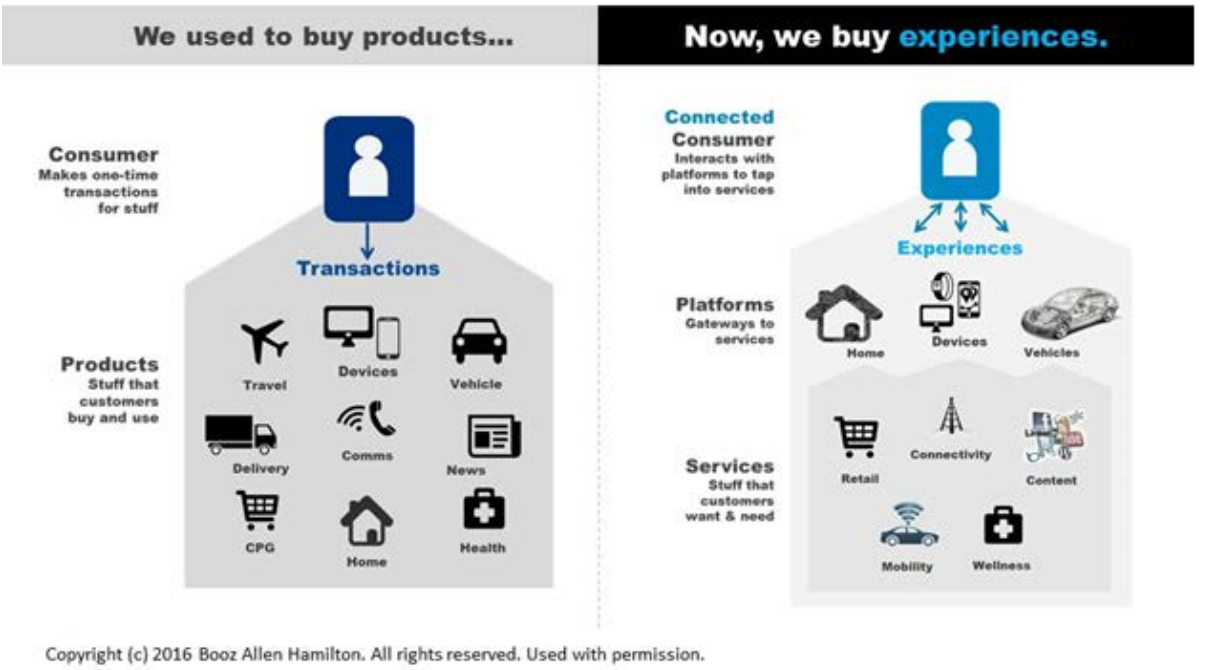

Figure 3.14. Information on Integrated Platforms[126]

Forthcoming shifts in production and simulation will further accelerate these trends in cost efficiency, flexibility, and innovation while adding capabilities to enhance personalization and drive greater integration of ICT into a range of materials, processes, and applications. For example, ubiquitous screens will enable more transient use and sharing of information, fostering more iteration and making personalization more accessible. 3D printing will dramatically reduce the costs of both test models and the production of unique materials and items, again enabling greater personalization and more iterative improvements. VR and AR will further enable iterative improvements in production, enabling simulated experiences in 3D-printed test models, as well as power new possibilities in personalized experiences. Lastly, advanced materials,

[126] Gary Barnabo and Alexandra Heckler. Booz Allen Hamilton, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* August 16, 2016.

including active nanotechnology, will shift what's possible in production, embedding connectivity and producing data across a range of new contexts and laying the groundwork for future leaps forward in interconnectivity as well as analytics, cognition, and autonomy.

Technologies discussed within this trend include:

- Ubiquitous screens;
- 3D and 4D printing;
- VR and AR; and
- Advanced materials science.

Figure 3.15 highlights these technologies as they were represented above in Figure 2.2.

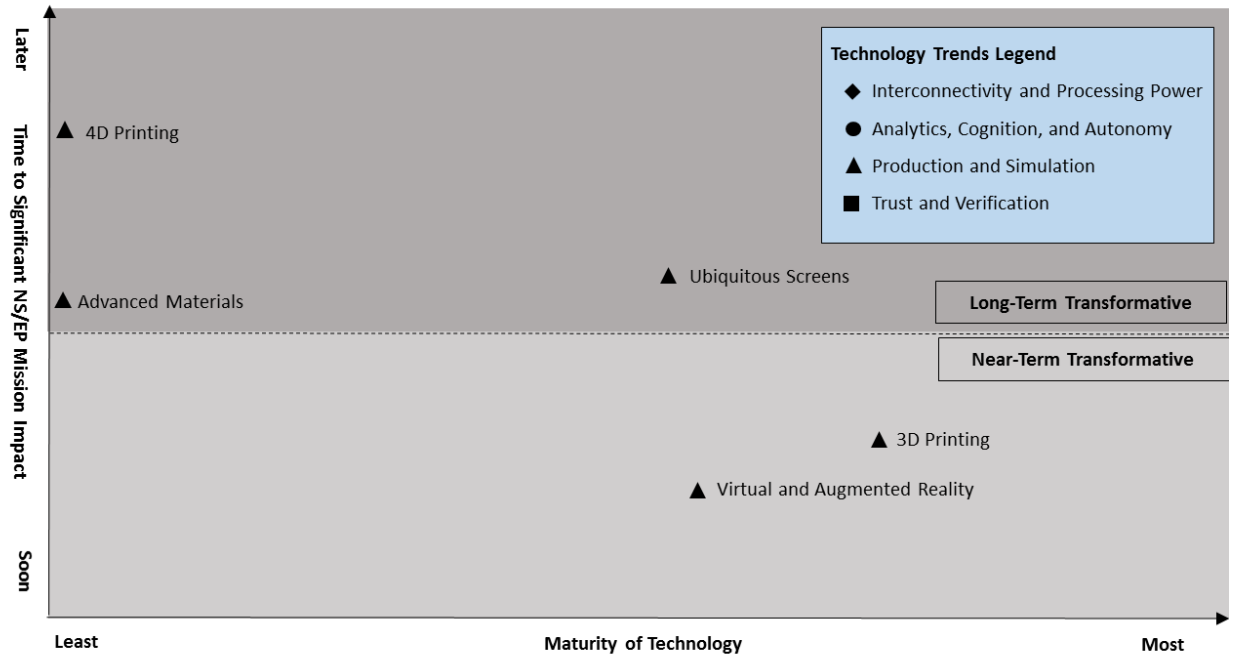

Figure 3.15. Production and Simulation

3.3.1: Ubiquitous Screens (Long-Term Transformative)

Introduction:

Today, more than 5 billion digital screens illuminate our lives, and digital display manufacturers will produce 3.8 billion new screens per year.[127] Screens fill our pockets, briefcases, workspaces, living room walls, VR goggles, gas station pumps, sides of buildings, and more, and we will

[127] Kevin Kelly. *The Inevitable: Understanding The 12 Technology Forces That Will Shape Our Future* (2016).

eventually put screens on any flat surface and consider them to be a primary mechanism for social interactions and information consumption.[128] Commentary on our screen-filled future often first reflects on our shift from newspapers to online news, from books to hand-held tablet readers; however, the long-term implications of ubiquitous screens extend far beyond the mechanisms of how we will read or the longevity of print media.

Ubiquitous screens are every flat surface that humans interact with in a dynamic and interactive way.

What are ubiquitous screens?

Discussion:

The dynamic flux of pixels will change how we access, share, interact with, and iterate on information within and among communities. For example, reading may become more social and increasingly dense, as ever-improving hyperlinking may make every book a continuously developing networked event.[129]

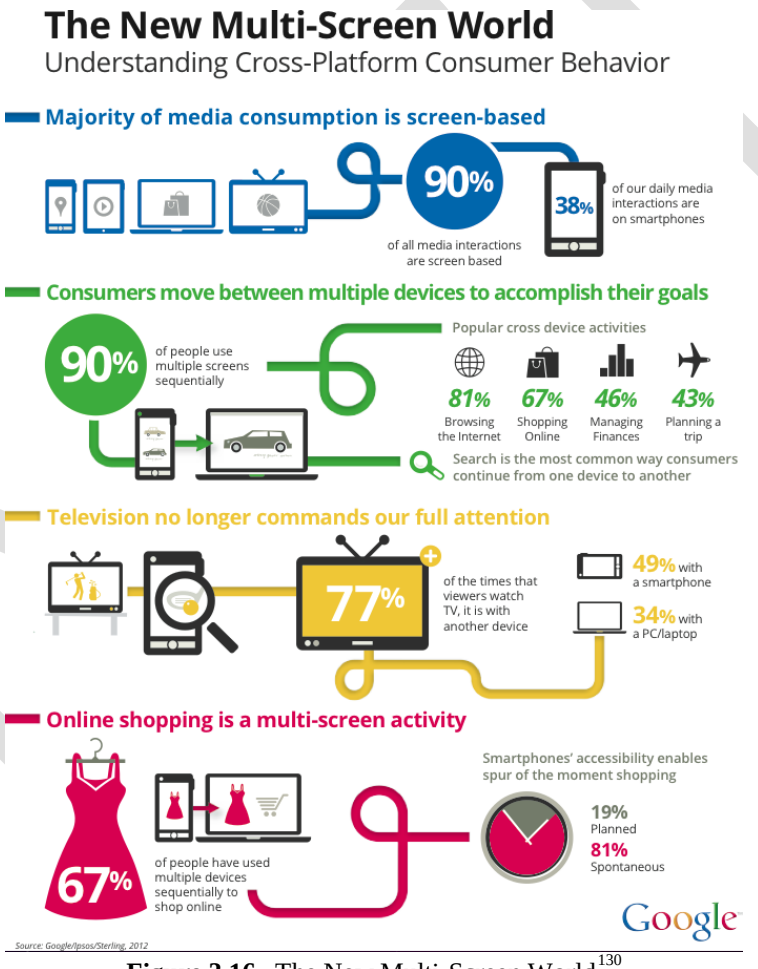

Figure 3.16. The New Multi-Screen World[130]

[128] Ibid.
[129] Ibid.
[130] Google. "The New Multiscreen World." Accessed on: April 7, 2017. https://www.thinkwithgoogle.com/infographics/multi-screen-world-infographic.html.

In addition, ubiquitous screens have the potential to make every interface personal and to display only the most relevant information in real-time. Moreover, interconnected, intelligent screens will be able to make such displays fluid as individuals move within a room or across environments. In that way, individuals could consume information without interruption or having to stare down at a hand-held device. As screens become a significant mechanism for interacting with others, they may also create new opportunities for such interaction, such as shared experiences in VR or AR.

3.17. Everything Can Be a Screen[131]

NS/EP Impacts:

In the context of NS/EP, ubiquitous screens, coupled with wide-ranging access to shared resources and communications, may help emergency responders gather the most relevant, up-to-date information as well as communicate with people and machines (e.g., AI). Intelligent, personalized screens could also share personalized information in emergencies, such as the location of family members, while limiting privacy concerns. In addition, in a national security context, connected smart screens could dramatically improve situational awareness.

Key Concepts	NS/EP Benefits	NS/EP Risks
Every flat surface becomes dynamic and interactive	• Greater access to shared resources and opportunities for information sharing and/or immediate cross-referencing to ensure responders have most relevant information • Personalized screens could share personalized information during disaster response	• Data security/privacy and data integrity challenges • Reliability issues • Authentication issues

[131] Liquid Newsroom. "Storytelling everywhere: Everything can be a screen." Accessed on: April 7, 2017. http://liquidnewsroom.com/#product.

3.3.2: 3D and 4D Printing (Near-Term and Long-Term Transformative)

Introduction:

Like many other technologies discussed here, approaches to and techniques for 3D printing, also commonly known as additive manufacturing, have been in development for decades. In recent years, though, advances have accelerated, with new applications and new materials being explored. According to a 2016 Wohlers Report, 3D printing has seen an average annual growth rate of 30 percent since 2011.[132] Moreover, growth is set to further accelerate, with Gartner Research estimating that by 2019, nearly 5.7 million 3D printers will be shipped annually, compared to an estimated 500,000 printers in 2016.[133]

Traditional manufacturing processes are based on the removal of raw materials to create final products. By contrast, 3D printing works by building a product layer by layer, using a technology designed for a specific type of material (e.g., selective laser sintering for metal alloys; fused filament fabrication for ceramics; and stereolithography for polymers). 4D printing creates 3D objects that change their shape over time in response to stimuli, such as heat, moisture, or light.

What are 3D and 4D printing?[134,135]

Discussion:

In the 2000s, the first 3D-printed kidney and prosthetic leg were developed, and in 2011, the first 3D-printed prototype car was developed. Throughout the 2010s, there have been advances in 3D-printed organs and prosthetics. Today, both large and small companies are increasingly using 3D printing to develop prototypes, including complex ones. For instance, SpaceX tested and retested their 3D-printed SuperDraco rocket engine for years before sending a rocket into space in 2015.[136] Efforts to develop and refine 3D-printed food, shoes, and a variety of customizable consumer products are ongoing. A major airline is even integrating 3D-printed material to help customize consumers' comfort on flights.[137]

While the technology has matured significantly over the past five years and costs have reduced dramatically, the production of low-volume and complex parts via 3D printing is economically viable only in cases where it reduces supply chain complexity and costs.[138] Still, the technology's versatile capabilities may eventually enable many diverse services, including the printing of human organs from stem cells and the printing of materials in space.

---

[132] Dr. Reinhard Geissbauer, Dr. Jorge Lehr, and Mr. Jens Wunderlin. *The Future of Spare Parts Is 3D.* January 20, 2017. https://www.strategyand.pwc.com/media/file/The-future-of-spare-parts-is-3D.pdf.

[133] Ibid.

[134] Ibid.

[135] Alice Klein. "4D Printing Makes Objects That Assemble Themselves When Heated." April 12, 2017. https://www.newscientist.com/article/2127713-4d-printing-makes-objects-that-assemble-themselves-when-heated/.

[136] Michael Abrams. "Top 6 Innovations in 3D Printing." February 2016. https://www.asme.org/engineering-topics/articles/manufacturing-design/top-6-innovations-3d-printing.

[137] Manya Jha. "5 Innovations in 3D Printing." July 18, 2016. https://www.entrepreneur.com/article/279243.

[138] Dr. Reinhard Geissbauer, Dr. Jorge Lehr, and Mr. Jens Wunderlin. *The Future of Spare Parts Is 3D.* January 20, 2017. https://www.strategyand.pwc.com/media/file/The-future-of-spare-parts-is-3D.pdf.

3D and 4D printing are projected to develop[139] in three stages:

1. In the immediate term, 3D printing will be increasingly used to develop spare parts, prototypes, simple medical devices, and other simple consumer products.

2. In the next five-to-10 years, 3D printing will be used to create products such as complex objects, complex foods, and advanced medical devices (including surgical devices, bone, advanced prosthetics, and vascular systems).

3. In the next 10-20 years, 4D printing will develop and emerge, enabling the engineering and design of physical matter that can change form and function in an intentional, programmable fashion.

As with near-term AI, as these technologies and industries advance, there will likely be efforts to standardize aspects of the various technological approaches, both in industry-driven forums and in other global technology standards forums. Again, as with near-term AI, as these efforts progress, the importance of U.S. Government investment in relevant standards forums will be critical to supporting innovation and security within the ecosystem.[140]

NS/EP Impacts:

Both near- and long-term developments in 3D and 4D printing may have significant impacts on the Government's NS/EP functions and missions. For instance, with access to a 3D printer, the ability to quickly develop and deploy a range of specialized products has the potential to support first responders in a variety of environments. In addition, 4D printing is of significant interest to national security communities. As one NSTAC briefer highlighted, the functional ability to embed smartness into an object so that it changes its material properties presents significant defense opportunities and risks, including the altering or unexpected emergence of weaponry.[141]

Key Concepts	NS/EP Benefits	NS/EP Risks
Manufacturing processes in which products are printed, layer by layer, enabling more iterative and flexible development and potentially enabling objects to change their shape in response to stimuli	• Ability to quickly develop and deploy a range of specialized products that may or may not change form in different environments • Simplified supply chain	• Lack of operational expertise • Lack of standards for materials or processes • The altering or unexpected emergence of a weapon

[139] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.
[140] Please refer to Section 5, *Recommendations*, for more information.
[141] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.

3.3.3: Virtual and Augmented Reality (Near-Term Transformative)

Introduction:

Like 3D printing, conceptions and early manifestations of VR and AR have been around for decades, but recent advancements make the technology well poised to be significantly impactful going forward. There are numerous VR headsets now available to consumers, and many potential applications, both practical and inspirational, are surfacing, including the use of virtual crime scenes in courtrooms (with video collected from drones), virtual test drives for marketing cars, simulated walking for paralyzed individuals, and training for surgeons. At least one auto manufacturer is already using VR to overlay virtual and physical models of cars with which their engineers can interact, eliminating the need to construct multiple physical models when dealing with design problems.[142]

VR is an immersive, computer-generated experience of a simulated environment. AR is a view of a real-world environment supplemented by computer-generated sensory input or synthetic or digital content (that may interact with real-world content in real time).

What are VR and AR?

Discussion:

While the growing ability to experience a simulated environment or to layer fiction onto reality has encountered technical and operational challenges to implementation, the technology will become widely adopted and much more advanced in the future, due in part to its ability to augment existing technologies.[143] Indeed, VR and/or AR will be the next major or dominant platform that hosts other services.[144] In other words, rather than doing work, ordering groceries, connecting with friends, or playing a game through a personalized screen in an autonomous car (see Section 3.2, *Analytics, Cognition, and Autonomy*), VR and AR will act as the platform for those activities. Moreover, in the future, VR and AR will be integrated into our lives in a more seamless way; for instance, VR will be viewable without a headset by multiple viewers—think real-time, full-color, 360-degree holograms. The timeline for widespread deployment of such future VR or comparable AR is speculative, but start-ups, early consumer wins (beyond gaming), and strategic partnerships on near-term approaches are driving advancements.[145,146,147]

VR and AR are poised to break through now, though the concept and basic underpinnings of the technology have existed for decades, because the price of relevant equipment has decreased rapidly with the commoditization of the smartphone and associated technologies. Put another way, VR and AR are breaking through because of advancements in processing power, analytics, and other technologies. However, there may still be some future challenges with deployment;

---

[142] Michael Floorwalker. "10 Innovative Applications for Virtual Reality." September 16, 2016. http://listverse.com/2016/09/16/10-innovative-applications-for-virtual-reality/.

[143] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.

[144] Kevin Kelly. *The Inevitable: Understanding The 12 Technology Forces That Will Shape Our Future* (2016).

[145] Devindra Hardawar. "Microsoft Has Big Plans for VR and AR in 2017." December 7, 2016. https://www.engadget.com/2016/12/07/microsoft-mixed-vr-holographic/.

[146] Tim Merel. "The Reality of VR/AR Growth." January 11, 2017. https://techcrunch.com/2017/01/11/the-reality-of-vrar-growth/.

[147] Alejandro Alba. "Augmented And Virtual Reality Might Be Everywhere In 2017." January 3, 2017. http://www.vocativ.com/387662/augmented-virtual-reality-2017/.

for example, the load and scale of data that will emerge with future VR and AR (such as, real-time, full-color, 360-degree holograms) will pose an immense burden on the telecommunications infrastructure. Such VR and AR would generate a full light field, which requires processing a tremendous amount of data in real time (and for which the necessary support infrastructure does not yet exist). 5G will likely be a significant development in enabling more widespread use of and future deployments of VR and AR.

As the technology evolves, VR and AR will have significant impacts, including unforeseen social developments that will be driven by human interaction with new technologies.[148] For instance, Pokémon Go, a mobile device application that allows users to interact with virtual images projected onto the device's camera based on the user's location, is an early indicator of the unforeseen social impacts that AR may have. The application prompted people to walk around outside, causing a variety of unexpected consequences, including both health benefits and physical safety concerns.[149]

As with near-term AI and 3D and 4D printing, as these technologies and industries advance, there will likely be efforts to standardize aspects of the various technological approaches, both in industry-driven forums and in other global technology standards forums. Again, as these efforts progress, the importance of U.S. Government investment in relevant standards forums will be critical to supporting innovation and security within the ecosystem.[150]

NS/EP Impacts:

There are significant NS/EP applications, opportunities, and challenges associated with VR and AR. Police and military training simulators have already significantly advanced with VR, as trainers can manipulate unique virtual scenarios in real time, giving officers personalized opportunities to gain experience and practice de-escalation and other techniques.[151] Future iterations of VR will further enhance organizations' training capabilities, including those of the DOD, due to the way in which it enables users to experience exercises at a deeper level. The potential for AR to impact officers and military personnel's experiences in conflict is also significant; an AR headset could integrate the ability to have greater awareness of surroundings, including, for instance, the ability to detect obscured metal. In the context of an emergency, VR or AR could be used to direct people, either routing them away from a crisis or, in a nefarious way, misdirecting people toward conflicts. In addition, as a platform, AR will increasingly be capable of providing users with tremendous amounts of information, though such capabilities may necessitate increased focus on effective methods of identification, such as biometrics (as discussed below), when all information about an individual is available instantaneously.[152]

[148] Alejandro Alba. "Augmented And Virtual Reality Might Be Everywhere In 2017." January 3, 2017. http://www.vocativ.com/387662/augmented-virtual-reality-2017/.

[149] Robert Ferris. "Pokemon Go's unintended consequences." July 11, 2016. http://www.cnbc.com/2016/07/11/pokemon-gos-unintended-consequences.html.

[150] Please refer to Section 5, *Recommendations*, for more information.

[151] Thomas Campbell. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.

[152] Ibid.

Key Concepts	NS/EP Benefits	NS/EP Risks
Immersive, computer-generated experiences that are either entirely simulated or that augment real-world experiences	• Realistic training • Ability to improve situational awareness (e.g. to detect obscured metal) • Ability to direct/route people in a more immediate, interactive way	• Lack of availability in combination with dependency (e.g., lack of ability to operate effectively without AR) • Integrity challenges, (e.g. risk of manipulation)

3.3.4: Advanced Materials and Material Science (Long-Term Transformative)

Introduction:

Significant discoveries and breakthroughs are being made at an accelerated rate in the fields of advanced materials, material science, and meta-materials. New polymers, graphene capabilities, ceramics, and nanomaterials are generating new possibilities in production—and will ultimately lead to flexible devices and communications, human augmentation, hyper energy efficient devices, and energy-generation devices. Energy efficiency and energy generation, in turn, will lead to new possibilities in integrating ICT, as the need to recharge will be reduced or even eliminated.

Advanced materials are a range of new materials that enable new capabilities, such as micro devices that are barely perceptible but join communications networks or other sensors that significantly augment human sensory functions.

What are advanced materials?

Discussion:

Some examples of developments in this field include super-lenses, optical filters, medical devices (including improved prevention, diagnostics, and care for soldiers),[153] extremely light and strong building materials (including those relevant for space exploration), lightweight protective materials,[154] smart solar power management, radomes, high-frequency battlefield communication, lenses for high-gain antennas, and improved ultrasonic sensors.

The Government supports a number of initiatives related to ongoing materials science and nanotechnology research. For instance, the Department of Defense, the National Institutes of Health, and the National Science Foundation partner with a variety of academic and other institutions on research.[155] NIST, a partner of both the National Strategic Computing Initiative and the Materials Genome Initiative, conducts modeling simulations to discover new materials that might have specific properties relevant to computing. NIST is also considering ways in which those materials can be engineered to overcome computing challenges, such as in support of neuromorphic computing, quantum computing, or data storage.

[153] Institute for Soldier Nanotechnologies. Accessed on: April 4, 2017. http://isnweb.mit.edu/soldier-medicine-prevention.html.
[154] Ibid.
[155] The National Nanotechnology Initiative. Accessed on: April 4, 2017. http://www.nano.gov/centers-networks.

NS/EP Impacts:

A wide range of capabilities, creating both opportunity and risk for NS/EP, include:

- Small and hard-to-detect electronic devices will be capable of being embedded within human beings or objects, enabled by low-power needs, power-generation attributes, massive data storage capacity, flexible circuits, and antennae. These devices could be used as sensors and communication systems.

- Low-cost, multispectral/hyperspectral sensors may permit consumer grade sensors that:
  - See through walls, into people, long distances, and at microscopic resolution;[156]
  - Hear selective and expanded auditory frequencies;
  - Hear and decode RF; and
  - Smell chemicals and detoxify chemical and biological agents.

- Miniature high performance computers at consumer prices will permit deep analytics at a level of personal customization previously available only to nations (similar to the evolution that has been seen in previous waves of computer technology).

- Long-range communications systems, leveraging quantum properties and terahertz waves among other developments, will enable new types of communications.

- Unmanned devices enabled by low-weight, high-strength materials will be capable of traveling long distances, with swarming abilities and substantial carrying capacity, and will be enhanced by the sensors, computing, and communications capabilities outlined above. (See more about unmanned/autonomous devices in Section 3.2.4, *Autonomous Vehicles.*)

Key Concepts	NS/EP Benefits	NS/EP Risks
A range of new materials that enable new capabilities, such as micro devices that are barely perceptible but can join communications networks or sensors that can augment human sensory functions	• More devices and connectivity to support greater analytics, cognition, and autonomy • Increased sensory capabilities (visual, auditory, olfactory) • Low weight, high strength materials	• The use of embedded or microscopic devices not visible to the human eye • The unexpected use of sensory amplifications (e.g., to see through walls, hear auditory frequencies beyond natural human range)

3.3.5: Summary: Production and Simulation Impacts

Building on ongoing shifts toward dynamic services and integrated platforms that enable a range of user experiences, forthcoming technologies, including ubiquitous screens, 3D and 4D printing,

[156] The National Nanotechnology Initiative. Accessed on: April 4, 2017. http://www.nano.gov/centers-networks.

and VR and AR will enable greater flexibility, more iteration, and greater personalization in production or simulation. Moreover, new materials will enable the production of both incredibly small, hard-to-detect devices, which can be widely integrated across new environments, and large, smart devices that benefit from low-weight, high strength materials. These shifts will fundamentally change how we make and interact with resources that, as discussed in the previous sections, will likely also enable greater connectivity and power and be powered by ever-increasing intelligence.

Each of these developments has implications for NS/EP operations. NS/EP situational awareness may be improved by ubiquitous, personalized screens, but new risks may also result from the integration of these technologies in the NS/EP context. With 3D and 4D printing, the changing nature of production and transformation of materials may significantly impact national security missions and how weaponry is developed, perceived, and used. VR and AR hold tremendous potential for military, police, and emergency responder training, but, especially in the context of AR, the possibility of manipulating information or filters may create new risks. Likewise, new materials will enable new possibilities in production and integration of ICT, which will power new capabilities and create new risks. As with interconnectivity and processing power and analytics, cognition, and autonomy, the challenge for the Government will be to leverage the promise of forthcoming technologies while maintaining awareness of and developing plans to mitigate the risks of evolving security threats.

3.4 Trust and Verification

Today, cybersecurity is an increasingly pressing issue for many organizations in both the public and private sectors. While estimates vary, the costs of cybercrime and economic espionage on the global economy are extraordinary.[157] Moreover, as increasingly sophisticated adversaries, including nation states, engage in more sophisticated acts of espionage and conflict, the risks to the continuity of critical operations and the continued trust in the innovation-advancing global ICT ecosystem also increase, along with the risks of kinetic effects.

Going forward, maintaining and strengthening trust in the global ICT ecosystem is fundamentally important, and both the public and private sectors must contribute to doing so. Businesses can do so by investing in security across the domains of people, processes, and technology and partnering with governments to share best practices and contribute to the articulation of Federal guidance. Governments can do so by establishing meaningful security policies and governance across the Federal enterprise,[158] incentivizing private sector adoption of cybersecurity risk management best practices, and facilitating the adoption of innovative technologies that may enable new approaches to mission performance and defense.

The NSTAC was directed to study the latter area—facilitating the adoption of innovative technologies that may enable new approaches to mission performance and defense. As the

[157] Hiscox Insurance estimated that, in 2016, cybercrime cost the global economy over $450 billion, and Deloitte in 2016 investigated the hidden or less visible costs of cyber attacks. Financial Tribune. "Cybercrime Cost Global Economy $450 Billion." February 9, 2017. https://financialtribune.com/articles/world-economy/59201/cybercrime-cost-global-economy-450-billion.

[158] NSTAC. *NSTAC Emerging Technologies Strategic Vision (ETSV) Letter to the President.* March 10, 2016. https://www.dhs.gov/sites/default/files/publications/Att%20%201%20-%20NSTAC%20Emerging%20Technologies%20Strategic%20Vision%20%28ETSV%29%20Letter.pdf.

NSTAC focuses on the Government's NS/EP mission, this report has described forthcoming technologies and possible applications and risks in that context. In this section, the NSTAC has focused its discussion on forthcoming technologies that substantiate or create new capabilities for managing cybersecurity risk. Ranging from cybersecurity platforms to quantum-resistant encryption, these technologies may be applicable to today's technology environment or responsive to the risks of forthcoming technologies. Either way, they are considered critical to maintaining and strengthening trust in the global ICT ecosystem. Additionally, technologies such as advanced biometrics and blockchain may help to not only build but also to substantiate trust through innovative approaches to verification.

Technologies discussed within this trend include:

- Cybersecurity platforms;
- Cybersecurity information sharing;
- Biometric identification and authentication;
- Blockchain; and
- Quantum-resistant encryption.

Figure 3.17 highlights these technologies as they were represented above in Figure 2.2.

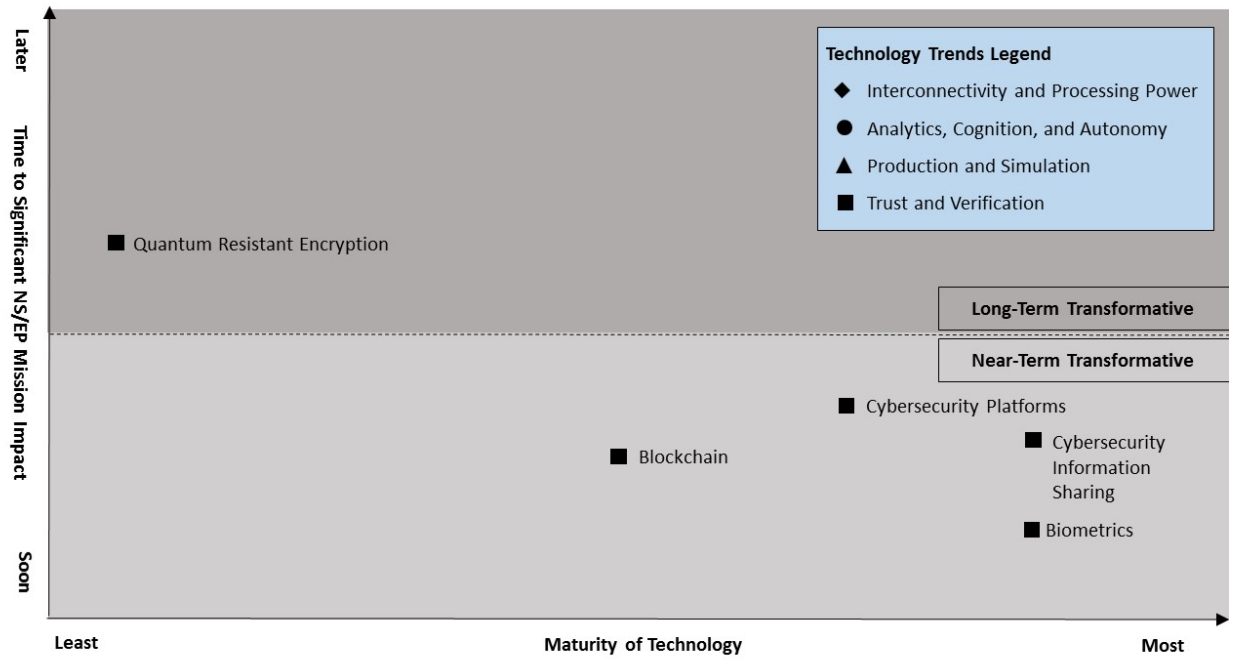

Figure 3.17. Trust and Verification

3.4.1: Cybersecurity Platforms (Near-Term Transformative)

Introduction:

As the cyber threat landscape has rapidly evolved and diversified, in part due to some of the current and emerging technology trends detailed throughout this report, the cybersecurity community has undergone a similarly significant evolution of consensus best practices for network defense. For example, from the beginning of Internet connectivity to the present, the industry has at various times coalesced around the cybersecurity best practice concepts of security by design, defense-in-depth, vendor-in-depth, best of breed, and security aligned to the 'Cyber Kill Chain' model.

One effect of this evolution—and the related evolution of network architectures—has been a dramatic proliferation in the number of cybersecurity companies and products, many of which are intended to address discrete security challenges but do not natively interoperate in a way that can holistically reduce priority cybersecurity risks across an organization's entire network infrastructure. This lack of technology orchestration and interoperability has become increasingly problematic as points of networked vulnerability have expanded due to technology trends such as virtualization, cloud computing, software as a service (SaaS) integrations, mobility, and IoT. This increased complexity of enterprise architecture without coordinated and interoperable security controls has ultimately created a dependence on one of the least scalable resources organizations have—people—to manually intervene to combat increasingly automated, machine-generated cyber attacks. The innovative solution that has emerged to address these orchestration challenges is the concept of cybersecurity platforms.

Cybersecurity platforms are a centrally managed and natively integrated collection of security architecture, tools, and processes that ensures consistent security to an entire computing platform.

What are cybersecurity platforms?

Discussion:

A cybersecurity platform is a centrally managed and natively integrated collection of security tools and processes that ensures consistent security across the entire computing environment. By definition, security platforms are largely integrated on the backend by a single cybersecurity vendor and feature fully interoperable technologies that are capable of automatic reprogramming based on newly discovered cyber threat information. In other words, if a threat is detected in one discrete component of an enterprise's network architecture (e.g., a single computer or 'endpoint'), then protections against that threat are automatically generated to protect the entirety of the network architecture, including all network, cloud, and endpoint environments. By definition, cybersecurity platforms must be capable of deploying preventive countermeasures regardless of where an enterprise's data resides or the deployment model of the network (e.g., whether on premises, in the cloud, or stored in third-party applications).

The ultimate promise of this maturing security model is its ability to simplify and automate network defense processes in a way that can keep pace with the highly automated nature of many modern cyber attacks. The platform model is a recognition that, in many instances, cybersecurity challenges are not primarily technological but instead a result of limitations in our ability to manage effectively the large sets of disparate security information generated by a complex set of security products. By combining these isolated products' respective capabilities in an integrated solution, platforms can reduce the complexity and burden of security correlation for the end user and provide the process cohesion necessary to ensure end-to-end security.

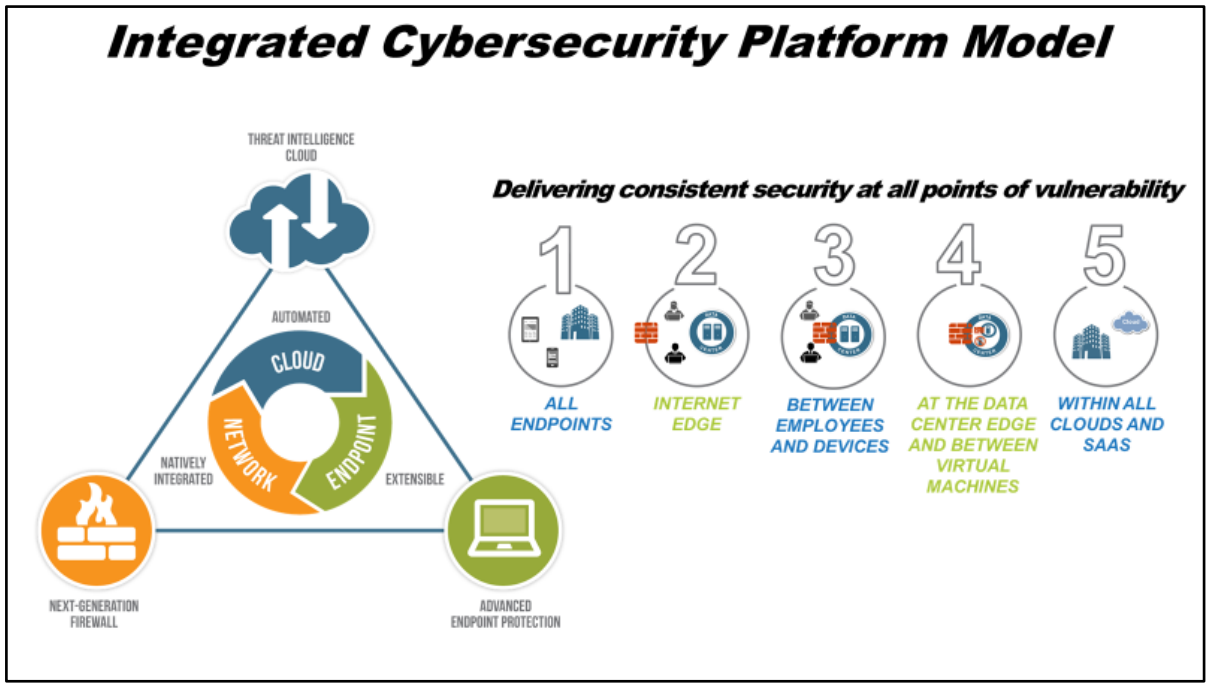

Figure 3.18. Depicts a cybersecurity platform model that comprehensively brings together defense of endpoints, networks, and cloud environments.

NS/EP Impacts:

The NS/EP implications of cybersecurity platforms are significant. Platforms provide a promise of reduced management complexity and consistent security, which can enable greater stability and reliability of Government operations and services. Because they provide consistent security regardless of the computing environment, platforms could incentivize governments to increasingly adopt SaaS-based or cloud technologies that often produce greater productivity and operational efficiencies. The increased process automation that comes with the security platform model also has the potential to positively impact the country's well-documented cybersecurity workforce deficit, including within NS/EP communities. For example, if the Government builds its workforce development strategies with a foundational understanding of current and emerging technologies that automate security processes such as cybersecurity platforms, then if can ensure that Federal agencies are recruiting and training cybersecurity personnel in a more targeted way for only those jobs that uniquely require a human's sophistication and critical thinking skills.

Undergoing this evaluation is likely to reveal that current cybersecurity workforce deficit estimates are artificially high because they assume unnecessarily complex, legacy defense models that require extensive human management and oversight. Many of these functions can be more efficiently addressed by AI and automated security technologies, and it is critical that the Government study this interrelationship in greater detail.

Key Concept/s	NS/EP Benefits	NS/EP Risks
A centrally managed and natively integrated collection of security architecture, tools, and processes that ensures consistent security to an entire computing platform	• Integration of security technologies to simplify and automate defense, better protecting networks and data • Potential to address workforce challenges by automating processes that have historically required inefficient human intervention	• Potential consolidation of risk exposure

3.4.2: Cybersecurity Information Sharing (Near-Term Transformative)

Introduction:

The inherently distributed nature of cybersecurity-related threats requires a more collaborative approach that leverages the unique capabilities, visibility, and authorities of private sector companies and governments. The emergence of new, innovative models for the automated sharing of cyber threat indicators to directly inform preventative action against cyber threats is one important manifestation of this collaboration.

Information sharing is a method for increasing visibility into attacker tactics and tools and for sharing security best practices that can help mitigate the impact of or thwart attacks. Today, information sharing is mostly limited to threat indicators, but future iterations could go further.

What is information sharing?

Discussion:

Just as adversaries are increasingly leveraging many of the technology developments outlined within this report to conduct increasingly automated, successful cyber attacks at minimal expense, so too are network defenders similarly leveraging these developments to increasingly automate defense through real-time sharing of cyber threat indicators. One such example of this new model of automation has been developed by the Cyber Threat Alliance (CTA), an information sharing partnership among private sector cybersecurity companies. [159]

[159] In one specific example of cyber threat information sharing among private sector entities, the CTA publicly shared extensive information about infrastructure and indicators associated with Cryptowall Version 3—a ransomware campaign that netted cyber criminals over $325 million. Shortly after the report's publication, Cryptowall criminals moved off the exposed infrastructure and produced new malware variants to form what security researchers named Cryptowall Version 4. In comparison to its predecessor, Cryptowall Version 4 generated a relatively insignificant amount of revenue ($18 million)—illustrating how automated sharing of cyber threat information can deter the severity of malicious activity by making it more expensive in terms of resources, time, and personal impact for adversaries to launch successful attacks.

The CTA uses a technically-integrated platform to share context-rich indicators, which members automatically convert to preventative countermeasures for deployment across their collective customer base. This represents a significant evolution from early forms of information sharing, which were often time-intensive processes that required a human to read, interpret, and manually create preventative controls based on technical threat indicators provided in a non-machine-readable format, such as a PDF or email. Such manual processes cannot scale to the speed and sophistication of the modern cyber threat environment.

Another recent trend has been collaboration between public and private sectors for specific operational activities enabled by cyber threat information sharing, such as law enforcement efforts to disrupt cybercriminal infrastructures or to combat ransomware.[160] For instance, public and private sector actors can collaborate to take down major botnets, working to disrupt and dismantle cybercrime groups.[161] In addition, law enforcement and two private sector partners launched an anti-ransomware initiative in July 2016, and it has been joined by 40 other law enforcement and private sector organizations.[162] Through collaboration, the initiative has disrupted multiple criminal operations.

NS/EP Impacts:

In the NS/EP context, automated information sharing and collaboration between public and private sector actors can help to increase situational awareness and inform response. In particular, advanced information sharing capabilities would likely be critical to waging an effective response to a cybersecurity event that resulted in an emergency situation. Information sharing could help not only to limit damage and restore ICT infrastructure functions but also to track perpetrators and inform global law enforcement responses.

However, information sharing may also serve to undermine such potential NS/EP benefits if the pool of information is accessed by an adversary. In that case, an adversary would have visibility into the range of techniques, tactics, and tools that are being tracked by collaborating public and private sector entities. In addition, an adversary may even have visibility into the techniques, tactics, and tools being used by defenders to limit or mitigate the impact of an attack. As such, protection of information sharing pools is critical.

[160] Through "ransomware," criminals use malware to access users' systems and then encrypt and hold their data or services ransom until the required payment is received. Estimates calculate criminals netting $1 billion through ransomware in 2016.

[161] Microsoft's Digital Crimes Unit regularly coordinates such efforts among public and private sector actors. Microsoft Digital Crimes Unit. "Digital Crimes Unit uses Microsoft data analytics stack to catch cybercriminals." March 2015. https://msdn.microsoft.com/en-us/library/dn949260.aspx Global law enforcement and private sector actors have also collaborated to disrupt the Beebone botnet. This botnet had infected tens of thousands computers across the world, with one estimate of 2.25 million unique samples of the malware spread across more than 195 countries. In this particular case, an eighteen-month investigation concluded in April 2015 to 'take-down' the infrastructure the malware used, dismantling a threat that was prevalent for a number of years.

[162] Europol. "No More Ransom: Law Enforcement and IT Security Companies Join Forces to Fight Ransomware." July 25, 2016. https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware

Key Concepts	NS/EP Benefits	NS/EP Risks
A method for increasing awareness of attacker techniques, tactics, and tools and for sharing of best practices that can mitigate the impact of attacks	• Increased visibility into security threats and actions to mitigate their impact	• Loss of information to adversaries, enabling them to change tactics or circumvent mitigations

3.4.3: Biometric Identification and Authentication (Near-Term Transformative)

Introduction:

Biometrics, which is the measurement of physical and behavioral traits for human identification, has largely been the domain of criminal forensics for about one hundred years, with increasingly widespread adoption over the last four decades for military, civil, and commercial purposes. Military applications include overseas counterterrorism red force identification as well as positive access control for local personnel accessing secure enclaves and stations. Civil purposes include physical access control at secure facilities, national-scale public benefits and electoral administration, and international travel security. In the consumer electronics world, cell phones with tiny fingerprint sensors have popularized biometrics for personal authentication, setting the stage for acceptance of biometric technology as a more secure and convenient method for computer network access.

Biometric identification and authentication is the use of measurable biological characteristics to determine the identity of a human that possesses those traits (identification) or to verify the identity of an individual (authentication).

What are biometric identification and authentication?

The most popular applications of biometrics provide identity protection and user convenience by delivering predicable and improved (and potentially faster) access to a desired benefit. Increasingly, these authentication experiences can be expected to have unobtrusive and natural user interfaces, such as facial recognition at a distance, iris at a glance, contactless fingerprint capture, speaker voice verification built into natural language speech interpretation systems, and signature or keystroke verification that does not distract from users' expected interaction with the environment. In the future, a car will likely detect a person's presence and verify his/her identity (as the car owner or requester) automatically before travel begins. The computer will verify an allowed user after being tasked to find and display a document or photograph.

Technology advances in facial recognition are also prominently appearing in social media channels, commercial cloud-based cognitive services, and retail solutions for consumer tracking and behavioral monitoring. Systems identify users and customize welcome routines and access levels, including recognizing states of mind (e.g., frustration or confusion) that can be addressed with additional customer support actions. Safe cities initiatives in many locales also feature surveillance for automated vehicle identification and video cameras, integrated in open spaces for public safety, that are being transformed into digital security surveillance platforms capable of automated human identification.

Discussion:

Criminal identification systems powered by biometrics have changed dramatically in the last decade. Historically, these systems relied on rolled ink-on-card fingerprints and low resolution mug shot photographs augmented by descriptions of scars, marks, and tattoos. Such systems were completely reliant on human fingerprint examiners for pattern classification and image minutiae matching, and the systems were only considered fast or effective when compared to the standards of the day. Today, computers perform thousands of fingerprint comparisons in seconds with subject galleries many times larger, and law enforcement is increasingly using DNA and iris scans for more accurate operations on larger populations.

Each more recent biometric has advantages and drawbacks. Fingerprint latent images often can be found at crime scenes and are the most familiar for forensic use, but automated matching can reach only a limited level of performance before manual experts are needed to resolve potential candidate matches. Facial images are frequently captured in surveillance video and can be recognized by people at distance, but automated matchers are highly sensitive to controlled lighting and, with the best performance, are several orders of magnitude below fingerprint matching. Iris codes—a monochrome bar code of the colored portion of the eye captured using near-IR light—rely on comparatively more expensive cameras and so have been collected for fewer individuals in the United States; however, they can deliver automated biometric accuracy that is several orders of magnitude better than fingerprints. DNA—using a small number of alleles to differentiate individuals rather than the full genome that is mapped for medical science—is relatively expensive and time-consuming to process, but it is highly unique. Its uniqueness results from its status as a genotypic rather than phenotypic characteristic, enabling use of familial similarities to identify individuals without necessarily collecting a sample from each individual person. DNA, then, is particularly relevant in the NS/EP context, as it can be used for disaster victim identification and in crime-fighting when there is a sample from a close relative but not one from the subject.

> E-passports are machine-readable documents that include an integrated radio frequency identification (RFID) chip containing passport information. Most e-passports contain at least a digitized face biometric complying with the standards issued by the International Civil Aviation Organization. A European Union regulation requires that passports issued by member states (except the United Kingdom and Ireland) contain a face and fingerprint biometric. The United States uses a database with over 100 million face images to perform de-duplication and watch list searches for known and suspected terrorists before issuing an e-passport containing a facial biometric. U.S. e-passports block RFID skimming (eavesdropping) when the passport is closed.

Specific use cases and performance versus cost trade-offs are more often drivers of designs and deployments than concerns with interoperability or future potential purposes. Operational biometrics used in civil systems may be unsuitable for large-volume, one-to-many identification if that is not a requirement, so situationally driven selection will result in choices such as signature (i.e., handwriting) dynamics, hand or fingertip vein geometry, voice verification, walking gait, or keystroke dynamics—all of which can work reasonably well for convenient one-to-one verification of willing subjects. When one-to-many identification or duplicate enrollment detection is required, then one of these may be augmented with fingerprints, iris scans, three-dimensional face recognition that uses structured light, or some combination of multiple enrollment modalities.

Risks from biometrics include:

- Invasion of privacy due to surreptitious involuntary capture;
- Unintended/unauthorized uses (including some DNA and retina scans that can reveal susceptibility to disease);

> At the 2001 Super Bowl, cameras at the entry gates captured images for comparison with digitized mug shots. Tampa Bay police reported that the system correctly identified 19 suspects. Public reaction included complaints due to lack of subject knowledge or consent. In the United Kingdom, overt surveillance is conducted by several million video cameras, including 500,000 in London alone, that scan pedestrians' faces against the photos of fugitives and terrorists. In 2005, a camera taped one of the subway bombers attempting to set off a backpack bomb, but the technology failed to identify the terrorists from watch lists before the bombing.

- Systems vulnerable to imposters or spoofing/replay/presentation attacks;
- Data integrity challenges, potentially resulting from either accidentally or maliciously edited data; and
- The ability of this technology to be used to inhibit freedom of movement and anonymity in public spaces.

These risks are relevant in the context of both widespread deployment and NS/EP functions and operations.

NS/EP Impacts:

Biometric identification and authentication have numerous current applications for NS/EP capabilities. Beyond criminal justice systems operated at the local, State, and national levels, there are specialized DOD tactical biometrics systems used for red-force identification and counter-improvised explosive device missions. There are also Department of Homeland Security (DHS) biometrics systems for counterterrorism, immigration control, and transportation security, where watch lists of suspected bad actors are used for fast one-to-many matching in order to screen visa applications, assess arriving international airline passengers, and pre-check domestic travelers into risk categories. As gallery sizes and exception handling have risen, systems have tended to move to multi-modal operations, adding, for example, palm print, facial, iris, DNA, and/or voice matching to what were once fingerprint-only systems. An essential element in criminal identification and other law enforcement systems is cross-platform interoperability to allow an interchange of data in standard formats. Civil biometrics applications have been used for years to secure access to sensitive facilities, protect electoral legitimacy in many countries, and provide identity management services as a public good in some societies.

Looking to the future, the form of AI known as deep learning (as described above) may produce dramatic breakthroughs in the accuracy and speed of facial recognition, even overcoming today's challenges with pose, obscured images (e.g., eyes only), and accurate pupillary location. There is general acceptance of biometrics for immigration control, and in the future, there will likely be wide-scale use for unobtrusively matching the identity of travelers entering and leaving the country and possibly for verification of travelers lacking normal identity documentation at airport security checkpoints.

A critical underpinning of any plan to overcome our society's cybersecurity challenges involves providing a means for trusting identities across networked devices that can serve all actors in our economy.[163] The NSTAC has commented on approaches to address this need with consumer-friendly identity management initiatives including biometrics and related technologies.[164] In line with recommendations by the NSTAC, progress has been made on potential foundations for effective identity management through the National Strategy for Trusted Identities in Cyberspace[165] and the development of open-source standards and specifications through the Fast Identity Online Alliance.

The touch sensors on consumer mobile devices and biometrics logon capabilities on today's desktop operating systems epitomize the way that user convenience can be enhanced to deliver faster access to a desired benefit while simultaneously preserving or even increasing security. The biometrics technologies involved are more difficult to spoof than traditional PINs or passwords and can provide the basis for two-factor authentication to enhance cybersecurity without reliance on auxiliary devices or out-of-band communications. The biometric performance of 3-dimensional face recognition and soon-to-be available iris recognition on affordable consumer laptops is sufficiently advanced and includes features that inhibit presentation attacks. A number of available application services use the sensors on virtually all smartphones to capture face and voice biometrics; these can be paired with other capabilities, including liveness detection, multi-modal fusion with location, and other information, contributing to transaction authentication and risk decision logic that can be applied selectively to various commercial settings, such as high-value financial transaction validation.

These trends suggest that biometric authentication may help play a significant role in the near future as a means to conveniently go beyond passwords to strengthen cybersecurity and protect against consumer identity theft. Per the latest NIST SP800-63A draft standards on identity verification, only a biometric comparison of the applicant to the identity evidence is sufficient to achieve superior identity verification.[166] It appears that the Government might have a critical role to play as a source to validate trusted identities at this level, taking advantage of existing Government services that already are depended upon for identity proofing, such as passport and driver's license systems with their associated facial image galleries.

---

[163] In this report, the recommendations include "a national public-private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management" and action items that "require that all Internet-based Federal Government services … require … strong authentication" and "the Government should serve as a source to validate identity attributes to address online identity challenges." NIST. *Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy*. December 1, 2016. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[164] NSTAC. *NSTAC Report to the President on Identity Management Strategy*. May 21, 2009. https://www.dhs.gov/sites/default/files/publications/NSTAC%20IDTF%20Report.pdf.

[165] EOP. *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*. April 2011. https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf.

[166] NIST. *DRAFT NIST SP800-63A Digital Identity Guidelines: Enrollment and Identity Proofing Requirements.* Accessed on: June 21, 2017. https://pages.nist.gov/800-63-3/sp800-63a.html. See table 5-3 on identity verification methods.

Key Concepts	NS/EP Benefits	NS/EP Risks
The use of measurable biological characteristics to determine or verify the identity of a human that possesses those traits	• Improved identification methods for national security purposes and emergency responders • Improved authentication and authorization to enable technology use	• Data security/privacy and data integrity challenges

3.4.4: Blockchain (Near-Term Transformative)

Introduction:

A blockchain is a constantly growing and distributed ledger of transaction records ordered into blocks with protection against tampering and revision. Unlike traditional database or directory technologies with a central administrator and coherent data storage, a distributed ledger provides a digital record of ownership that is replicated among numerous nodes in a peer-to-peer network. A consensus mechanism is used to authenticate and validate a value or transaction on the blockchain—such that the distributed ledger technology does not need to trust or rely on a central authority. Each transaction is uniquely signed with a private key by the initiator, and the blocks are chained together by referring to the unique hash of a block's predecessor.

Blockchain is a way to structure data; a digital ledger of blocks of transactions, enabling entities to agree on the history of a system and its current state without need for a central authority to confirm transactions.

What is a blockchain?

In contrast to current systems with centralized processing, there are two basic decentralized blockchain application models and consensus protocols: public blockchain that is permission-less (on an open network), and private blockchain that is permissioned (on a private network). Use cases for both of these categories of blockchains are entering the market and will evolve significantly over the near and long term; indeed, the process of blockchain adoption will likely be gradual and steady, not sudden, as waves of technological and institutional change gain momentum.[167] Who uses blockchains and how they do so will be determined by a range of inputs, including customer demands, risk management considerations, compliance obligations, and the continuing evolution of technology.

Still, the NSTAC considers blockchain a near-term technology because applications have already emerged and will continue to do so in the next five years. The best known public blockchain, called Bitcoin, provides pseudo-anonymity for digital currency exchange (based on a paper published in 2008 titled "Bitcoin: A Peer-to-Peer Electronic Cash System").[168] Looking beyond its initial use as a virtual currency, the underlying protocol of Bitcoin and the protocols of other blockchains allow developers to build a technology solution for markets where participants need to agree on some form of consensus behavior in otherwise unsecure and untrusted environments.

[167] Marco Iansiti and Karim Lakhani. "The Truth about Blockchain." https://hbr.org/2017/01/the-truth-about-blockchain.

[168] Satoshi Nakumoto. "Bitcoin: A Peer to Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.

For example, rather than simply using a blockchain protocol to record financial transactions, developers are now using blockchain to build programmable behavior for multiple parties.

Discussion:

Many uses of blockchains have been imagined as the vehicle for an Internet of value, but the blockchain technology will also have broader implications; indeed, understanding of the potential applications for and the security implications of this foundational technology and its various consensus mechanisms is in the early stages and still evolving. In the financial services industry, blockchain and distributed ledger technology provide a means for secure and efficient decentralized instruments of trust between parties to a contract, such that a financial transaction may be self-validating to allow immediate settlement. There are also applications in energy,[169] healthcare, and music distribution and platforms from dozens of technology innovators.[170] One of the more interesting potential applications is how blockchain fits into the future of digital identity.[171] It could also be the technology that provides the mechanism to reinvent the Web for better integrity and/or privacy.[172] In the NS/EP context, there could be many potential applications for, and risks related to, a technology that enables the sharing of information in a trusted, pseudo-anonymized way.

As this technology approaches greater maturity, and its potential advantages as a scalable mechanism for efficiently sharing trusted transaction information are applied to new contexts, there may be numerous applications relevant to many industries. For public sector agencies, there are applications in benefits administration, as it can reduce friction in terms of both transaction processing cost and cycle time while simultaneously providing built-in mechanisms to reduce fraud. For example, the Estonian government is using blockchain technology to ensure the integrity of its records, logs, and systems.[173] In addition, the State of Delaware recently began using blockchain technology to help automate and maintain the way the state manages uniform commercial code filings.[174]

NS/EP Impacts:

The Government should explore blockchain for digital identity management within both closed domains (e.g., the NS/EP community) and in Government-to-industry and Government-to-citizen interactions where it has the potential to protect identity and enhance personal privacy without the restrictions typically found in predecessor technology schemes such as public key infrastructure. However, commensurate with the value of the information and transactions being

[169] Jonathan Mather. "The Energy Blockchain – Believe The Hype, Just Don't Forget The Physics." February 22, 2017. http://berc.berkeley.edu/energy-blockchain-believe-hype-just-dont-forget-physics/.

[170] E.g., the Sawtooth Lake distributed ledger platform from Intel and the way that Microsoft is building interoperability among various blockchain platforms and tools that run on its Azure cloud service.

[171] Bryan Yurcan. "How Blockchain Fits Into the Future of Digital Identity." April 8, 2016. https://www.americanbanker.com/news/how-blockchain-fits-into-the-future-of-digital-identity.

[172] Tom Simonite. "One Startup's Vision to Reinvent the Web for Better Privacy." January 13, 2017. https://www.technologyreview.com/s/603352/one-startups-vision-to-reinvent-the-web-for-better-privacy/.

[173] Iyke Aru. "Estonian Government Adopts Blockchain to Secure 1 Mln Health Records." March 9, 2016. https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records.

[174] Martin Ruubel. "Blockchain-Enabled Cloud: Estonian Government selects Ericsson, Apcera and Guardtime." August 28, 2016. https://guardtime.com/blog/blockchain-enabled-cloud-estonian-government-selects-ericsson-apcera-and-guardtime.

protected, systems that rely on blockchain technologies should be scrutinized at high levels. As with any security technology, lifecycle planning should include provisions for improved hardening over time since evolution will be driven by the identification of technical and operational risks. Beyond the public sector, critical infrastructure industries and an increasing portion of the U.S. economy may become dependent on blockchain technology. In this case, it will also be critical for the Government to help by informing users and other reliant parties on the risks and approaches to protect these systems.

Key Concepts	NS/EP Benefits	NS/EP Risks
A digital ledger of blocks of transactions, enabling entities to agree on the history of a system and its current state without a central authority	• Check on data integrity • Sharing of cybersecurity threat information in a more trusted way • Widespread digital identity systems	• Widespread dependency • Post quantum, the integrity of blockchain ledgers may be at risk

3.4.5: Quantum-Resistant Encryption (Long-Term Transformative)

Introduction:

As discussed in Section 3.1.5, *Quantum Computing,* today's commonly used public-key encryption algorithms, which form "the bedrock of most modern data protection," will be easily broken by a quantum machine.[175] Quantum computing has not been proven to break every public-key encryption algorithm, but it does break those based on integer factorization, the discrete logarithm problem, and the elliptic curve discrete logarithm problem—which represent the full array of public-key encryption algorithms in common use.[176] Notably, quantum computers enable better attacks against symmetric cryptographic algorithms too, but such attacks can be blunted by moving to larger key lengths—"a comparatively easy change."[177] Although no one knows when a quantum machine will be deployed, this risk to public key (asymmetric) cryptography is extremely palpable and severe. As soon as a quantum machine is deployed, a significant amount of

Quantum-resistant encryption is a set of deployed public key encryption algorithms that are resistant to being broken by a fully functioning quantum computer.

What is quantum- resistant encryption?

[175] Dan Goodin. "NSA preps quantum-resistant algorithms to head off crypto-apocalypse." August 21, 2015. https://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/.

[176] In 1994, Peter Shor developed the first quantum algorithm, "Shor's algorithm," that demonstrated that, in conjunction with a sufficiently powerful quantum computer, it would break public-key encryption based on integer factorization.

[177] Nicole Kobie. "The Quantum Clock Is Ticking on Encryption – and Your Data is Under Threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption. As a concrete example, the AES symmetric encryption algorithm has both a 128-bit key and a 256-bit key mode (where the secret keys are 128- or 256-bits long, respectfully). Today we might use AES-128, and a brute force attack on AES would take about 2^128 time. With a quantum computer, we can do the same attack in time equal to the square root of that effort, of 2^64 time—which is too little resistance. As such, the response to quantum computers is to move to AES-256 with 256-bit keys and a quantum attack complexity of 2^128. AES-256 is already widely supported, so there's little focus on this aspect of the problem.

public and private sector data will be at risk; the public keys used to secure Government data, online banking, email, and much more "have an expiration date that coincides with quantum's birthday."[178]

Discussion:

The seriousness of the risk to public key cryptography posed by quantum computing is significantly elevated due to the extended time frame that will be necessary to develop, standardize, and deploy quantum-resistant encryption. While efforts to develop quantum-resistant encryption are ongoing, and increasingly coalescing around a few approaches (i.e., lattice-based, isogeny-based, hash-based, code-based, and multivariate polynomial solutions),[179,180] before being standardized and widely deployed, encryption algorithms undertake a long process of public vetting. According to NIST, developing standards for post-quantum cryptography "will require significant resources to analyze candidate quantum-resistant schemes, and will require significant public engagement to assure trust in the algorithms NIST chooses to standardize."[181] In addition to building public trust, NIST's evaluation and standardization process also builds expert and industry confidence.[182] However, some of this process may be accelerated by the approach that NIST is taking in its ongoing competition, which will be further discussed below. The competition requires that each submission include both a reference implementation and an optimized implementation of the proposed algorithm, demonstrating the algorithm's operation.[183]

Even after implementation has been demonstrated and standardization has occurred, deploying winning algorithms into existing security protocols can also be an extremely lengthy process; outdated, vulnerable encryption algorithms cannot be easily replaced by newer, quantum-resistant algorithms. Rather, cryptographic agility, which occurs when applications or protocols can accommodate the insertion of different algorithms or suites of algorithms, is difficult and must be thoughtfully engineered by design.[184] In addition, protocols must be able to accommodate variations in storage requirements; for example, because most in-development quantum-resistant encryption algorithms have larger key sizes than the algorithms they will replace, various protocols, including the Transport Layer Security (TLS) protocol,[185] may need to

---

[178] Nicole Kobie. "The Quantum Clock Is Ticking on Encryption – and Your Data is Under Threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption.

[179] NIST. *Report on Post-Quantum Cryptography.* February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[180] Crypto Forum Research Group. *Draft: Hash-Based Signatures.* September 6, 2017. https://www.ietf.org/id/draft-mcgrew-hash-sigs-06.txt. Notably, the Internet Engineering Task Force (IETF) is already working on standardizing one hash-based signature scheme, which will not be a drop-in replacement for a traditional public-key signature scheme but will nevertheless have some uses.

[181] Ibid.

[182] Nicole Kobie. "The quantum clock is ticking on encryption – and your data is under threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption.

[183] NIST. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process.* http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf

[184] Internet Engineering Task Force. *Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms.* November 2015. https://tools.ietf.org/html/rfc7696.

[185] TLS, which provides communications security over computer networks, is widely used; for example, the use of TLS to secure HTTP traffic constitutes the HTTPS protocol.

change.[186] Moreover, organizations, including both the public and private sectors, must invest in new technology with crypto agility and/or quantum-resistant encryption rather than wait for current technology to complete its replacement lifecycle. Past transitions from one cryptographic algorithm to another have taken from five-to-twenty years; for instance, some organizations are only now starting to transition to elliptic curve cryptography, which NIST began advising them to do in 2000.[187]

According to a 2016 NIST publication, some engineers predict that within the next 20 years, sufficiently large quantum computers will be built to break essentially all currently deployed public key cryptography, but historically, "it has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take a significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum-resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information systems to be able to resist quantum computing."[188] In 2015, the National Security Agency (NSA) began advising U.S. agencies and businesses to transition to quantum-resistant cryptography and publicly expressed its commitment to working to develop a new suite of algorithms.[189]

In 2016, NIST rolled out its strategy for supporting the development of post-quantum cryptography and began accepting proposals for quantum-resistant public key encryption.[190,191] As part of the competition referenced above, NIST will accept proposed encryption algorithm submissions until November 2017 and will ask eligible submitters to present their ideas in 2018. Then, NIST will allow the proposals to be subject to 3-to-5 years of public scrutiny and evaluation before they are standardized; NIST anticipates that it will select "winning" algorithms in 2023-2025, and organizations should be prepared to transition to new algorithms in 10 years.[192,193] Notably, even if NIST successfully standardizes new, quantum-resistant algorithms by 2025, network and application protocols are modified in parallel, and organizations in both the public and private sectors are prepared to deploy those algorithms by 2030 (an aggressive

---

[186] NIST. *Report on Post-Quantum Cryptography.* February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[187] Nicole Kobie. "The quantum clock is ticking on encryption – and your data is under threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption. Past hash-function transitions (both MD5 and SHA-1) also demonstrate the likelihood of protracted transition timelines.

[188] NIST. *Report on Post-Quantum Cryptography.* February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[189] Dan Goodin. "NSA preps quantum-resistant algorithms to head off crypto-apocalypse." August 21, 2015. https://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/.

[190] NIST. *Report on Post-Quantum Cryptography.* February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[191] NIST. "Announcing Request for Nominations for Public-Key Post-Quantum Crypotgraphic Algorithms." December 20, 2016. https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms.

[192] NIST. *Report on Post-Quantum Cryptography.* February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

[193] Dustin Moody. *Update on the NIST Post-Quantum Cryptography Project.* June 2016. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2016-06/2_post-quantum_dmoody.pdf.

timetable relative to past deployments), if a sufficiently powerful quantum machine is accessible by 2032,[194] then that still means that data encrypted at least two years before may be decryptable.

NS/EP Impacts:

As discussed in the above section on quantum computing, there are clear national security equities impacted by the deployment of this technology. Until it is protected by quantum-resistant encryption, any data protected by commonly used public key encryption algorithms, whether at rest or in transit, will be vulnerable. If such data, encrypted using pre-quantum algorithms, has been collected and is held until a sufficiently powerful quantum machine can be applied to it, then it can be decrypted. Until quantum-resistant encryption is implemented, all collected (and persistently held) data, including Intelligence Community communications and data, could be readable in the foreseeable future. For instance, if quantum-resistant encryption is sufficiently deployed to protect Intelligence Community systems in 10 years, and an adversary obtains a sufficiently powerful quantum machine in 15 years, then encrypted intelligence more than five years old and in the adversary's possession could be accessed, a time frame much sooner than the minimum time allotted by the Government for automatic declassification.[195]

Key Concepts	NS/EP Benefits	NS/EP Risks
A set of deployed public key encryption algorithms that are resistant to being broken by a fully functioning quantum computer	• Ability to protect communications and data from decryption	• Lack of visibility into communications and data protected by post-quantum encryption

3.4.6: Summary: Trust and Verification Impacts

The fourth and final major trend examined by the NSTAC was the overarching trend of trust and verification. As cybersecurity challenges resulting from the use of current technologies are ongoing or even expanding alongside greater adversary investments, forthcoming technologies discussed in this report may mitigate some of those threats while also potentially creating new risks. In addition, as discussed in this section, there are ongoing efforts to develop new technologies that address current and future risks.

The NS/EP impacts of these emerging and expected trust and verification technologies, including cybersecurity platforms, information sharing, advanced biometrics, blockchain, and quantum-resistant encryption, are potentially significant. These technologies may help Government agencies that manage NS/EP functions mitigate existing risks, make investments to dramatically reduce risks, and prepare for expected technology developments, including quantum computing.

[194] Nicole Kobie. "The Quantum Clock Is Ticking on Encryption – and Your Data Is Under Threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption. Dr. Michele Mosca, deputy director of the Institute for Quantum Computing at the University of Waterloo, Ontario estimates a one-in-seven chance that some fundamental public-key crypto will be broken by quantum by 2026 and a one-in-two chance of the same by 2031.

[195] Department of Justice. "Declassification Frequently Asked Questions." September 13, 2016. https://www.justice.gov/open/declassification/declassification-faq.

4.0 IMPACTS ON NS/EP FUNCTIONS AND MISSIONS

The NSTAC cannot imagine all the ways that the technologies reviewed in this report will individually or collectively affect NS/EP functions and missions. However, for each technology, we have identified specific impacts and described them at a level of specificity consistent with what the current status of the technology allows. For most areas, the NSTAC noted that the impacts are double-edged, bringing potential NS/EP benefits but also creating new threat vectors. For example, advanced UAVs could greatly enhance response capabilities in the event of a natural disaster, but they could also be used to attack physical infrastructures. For a summary of technology-specific NS/EP impacts, see Appendix D, which includes a series of charts that highlight NS/EP benefits and risks for each technology.

In addition, the NSTAC discerned impacts that cut across emerging technologies. This section delineates three broad, evolutionary themes and examines impacts that each could have across the spectrum of the Government's NS/EP mission.

4.1 ICT Architecture That is Data Rich and Distributed

Theme: Technologies (primarily SDN/NFV and IoT, supported by ubiquitous networks, including 5G) will transform the ICT architecture into a more data robust and distributed form. Fully deployed IoT will vastly increase the amount of data generated by people and infrastructures. Nearly every part of the ICT architecture, as well as many other infrastructures, will generate and retain big data. The data will be housed and processed in virtual networks built on a widely dispersed and generic physical infrastructure.

NS/EP Impacts:

- NS/EP functions will be enhanced through the greater situational awareness available in a data rich environment. The Government could leverage the available data (assuming it is properly positioned to do so) to improve its NS/EP planning and response activities.

- The distributed and virtual nature of the new architecture could make infrastructures, particularly communications infrastructures, more resilient and could enhance restoration efforts in the aftermath of a catastrophic event. However, the same distributed and virtual feature of the new architecture will complicate defensive NS/EP planning, as the physical location of key infrastructures becomes more difficult to determine.

- The Government will be able to use the new architecture to improve its own capabilities and to render its own infrastructures more resilient and secure. Similarly, the Government will be able to improve general operations by leveraging new stores of data. However, the Government's adoption of the new architecture must be carefully planned and must contemplate the effects on legacy systems (including the indirect effects of diverting resources to the newer technologies).

- The new architecture will enable new approaches in cybersecurity and distributed verification platforms (like blockchain).

4.2 A World in Which the Physical, Cyber, and Virtual Merge

Theme: Deployed IoT, ubiquitous networks, and distributed infrastructures will further integrate control of the physical environment into the ICT architecture. At the same time, ubiquitous screens, VR and AR, and 3D and 4D printing will render geography less relevant in business and social interactions.

NS/EP Impacts:

- On-demand production of needed supplies to support NS/EP capabilities could be accomplished with standardized materials and sufficient operational expertise.

- Smart infrastructures will enhance NS/EP capabilities in crisis situations. Evacuations, response operations, and recovery will all benefit from physical infrastructures that can be controlled and aligned with emergency operations. The same infrastructures, however, will enable cyber attackers to more easily achieve kinetic effects.

- Cybersecurity will become a major challenge in this context, particularly if IoT control systems are not deployed securely.

- VR and AR will enhance training for NS/EP functions and could allow for the dispersal of critical functions from vulnerable locations.

- The connectivity required by these technologies will make great demands on the communications infrastructure, and NS/EP functions and priorities will need to be properly supported in that environment.

4.3 Rapid, Radical Transformation

Theme: Just over the horizon are advances that will radically disrupt our technical and social environments. Quantum computing, advanced AI (i.e., truly autonomous machines), and developments in material science (i.e., enabling nanotechnology, biomorphic computing, etc.) will all re-form foundational aspects of our world.

NS/EP Impacts:

- Quantum computing could undermine all widely deployed public key encryption, with severe implications for national security equities and economic systems. NS/EP and other critical systems will need to be defended (with quantum resistant encryption) if the United States is not the first to acquire quantum capabilities.

- Advanced AI may greatly enhance NS/EP functions, particularly as AI and autonomous machines can be deployed in emergency response situations.

- AI will also enhance both cyber and physical security capabilities, though adversaries will eventually have access to the same tools.

- The arrival of AI and autonomous machines will raise issues about the appropriate rule sets to govern the behavior of these assets, particularly with respect to AI decision-making that could affect human life.

- AI and autonomous machines could significantly disrupt the human labor force and potentially have broad social effects.

- Each of these radically transformative technologies will create new demands on the Government's own labor force and will render many existing qualifications and training programs obsolete.

5.0 RECOMMENDATIONS

Based on our findings across technologies and trends, the NSTAC developed a set of recommendations, highlighting opportunities and areas of concern. While the recommendations are not listed in order of priority or importance, they are organized under three headings:

- "High-priority actions" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for near-term technology developments;

- "Strategic opportunities" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for long-term technology developments; and

- "Cross-technology imperatives" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for multiple near- and long-term technology developments.

High-Priority Actions:

- **Develop a Strategic Plan to Modernize ICT Network Architecture in Support of the Government's NS/EP Mission.**

    - The Government should leverage shared infrastructure and common services, including cloud computing and SDN/NFV, as well as a more integrated approach to incorporating innovative technologies across the Government.

    - The Government should develop a policy and plan, similar to that developed for cloud computing, for the efficient acquisition and implementation of SDN and NFV in Federal networks. In doing so, the Government should assess which networks should be slated for accelerated upgrade or replacement, and oversight should be established to ensure that critical upgrades and required changes are made with sufficient urgency.

    - The Government should evolve existing Federal and critical infrastructure protection guidance to incorporate SDN/NFV developments. In particular, in

consultation with infrastructure operators, the Department of Homeland Security should: (1) review the effects of SDN/NFV on the existing critical infrastructure taxonomy; and (2) support NS/EP planners in identifying key virtual assets in critical infrastructure and leveraging SDN/NFV for response and recovery efforts.

- The Government should streamline the regulatory approval process for 5G technology to facilitate its rapid deployment and enable other technology developments.

- The Government should modernize its procurement processes to achieve the level of agility demanded by the emerging technology environment. In particular, the Government should consider establishing a special fund that agencies can use to replace legacy information technology systems[196] that pose unacceptable cybersecurity risks; accelerating agency use of existing funding for small-scale testing or piloting of shared services or new technologies; and supporting the development of dedicated, cross-agency procurement teams that are knowledgeable about forthcoming technologies and skilled in agile processes.

- **Promote and Prepare for IoT Capabilities that Agencies Can Leverage to Advance Their NS/EP Missions.**

  - The Government should direct the Office of Management and Budget to require agencies to: (1) assess and document IoT capabilities that currently support and/or are planned for support of NS/EP functions, considering interconnections and interdependencies that may be introduced; and (2) develop plans to manage security risks created by current and future IoT deployments. The plans should recognize the fast pace of IoT innovation and that some parts of the IoT ecosystem may, at least initially, prove very hard to secure (e.g., due to the number of devices and lack of security standards). As a result, Government plans must be adaptable, and the Government must be able to provide NS/EP services even if IoT functions or capabilities are degraded.

  - The Government should sustain and, where relevant, strengthen investments in facilitating Government and industry coordination to address IoT opportunities and risks, including by: (1) continuing to support public-private partnerships being pursued by the Department of Commerce (DOC);[197] and (2) tasking the DOC to continue advocating for industry-led approaches and consensus-based standards by establishing a Government and industry standing body to collaborate on and leverage the various industry IoT consortia guidelines that are being developed, updated, and maintained to manage IoT deployment risks.

- **Improve Manageability, Security, and Resilience of Current and Future ICT.**

[196] The White House. "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[197] National Telecommunications Industry Association (NTIA). "Internet of Things." Accessed on: April 4, 2017. https://www.ntia.doc.gov/category/internet-things.

- As part of its policy and plan for the efficient acquisition and implementation of SDN and NFV in Federal networks, the Government should address the security of SDN/NFV technologies. In particular, the Government should consider SDN/NFV control plane issues as well as other cybersecurity and supply chain security issues relevant to the new technology.

- The Government should energize public-private initiatives focused on improving identity management.[198] In particular, the Government should require strong, multi-factor authentication for access to Government networks and citizen-facing services. Additionally, the Government may consider serving as a source for the private sector to validate trusted identities, including in the context of biometrics.

- The Government should facilitate cross-agency efforts to evaluate NS/EP applications for blockchain technology, including the sharing of trusted transactions and other data, such as digital identity or cybersecurity threat information. The use of blockchain will likely be particularly relevant when the integrity of transactions or data is critical. In addition, the Government should facilitate cross-agency efforts to evaluate the potential risks of using or relying on blockchain technology for NS/EP applications.

- **Invest in Government Participation in Global Technology Standards Forums.**[199]

  - 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 centrally coordinate its engagement in global technology standards forums at the executive leadership and interagency levels. In addition, it should develop mechanisms for regular collaboration with the private sector and other governments, enabling strategic prioritization and investments.

Strategic Opportunities:

- **Position the U.S. Workforce to Create, Use, and Manage 21st Century Technology by Investing in Education and Training Programs.**

  - The Government should invest in education and training programs that enable the Government, as well as the broader U.S. workforce, to be prepared to leverage new technologies and lead ongoing innovation. Special attention should be

[198] The White House. "The National Strategy for Trusted Identities in Cyberspace." Accessed on: July 5, 2017. https://obamawhitehouse.archives.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace.

[199] National Institute of Standards and Technology (NIST). "NISTIR 8074 Volume 1: Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity." Accessed on: July 5, 2017. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf. NIST. "NISTIR 8074 Volume 2: Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity." Accessed on: July 5, 2017. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf. NIST. "Comments on the 8/10/15 Draft NISTIR 8074, Volumes 1 and 2." Accessed on: July 5, 2017. https://www.nist.gov/itl/comments-draft-nistir-8074-volumes-1-and-2.

focused on programs that address developments in AI and machine-to-machine communication.

- The Government should invest in re-training programs and employment services for disciplines that may be affected in the near term by shifting labor needs.

- **Assess New Governance, Legal, and Operational Challenges Resulting from Emerging AI, Autonomous Devices/Systems, and Materials Science Advances.**

  - The Government should drive and/or support research to achieve greater clarity around the impacts of software-based decision-making by autonomous systems, including both military and commercial systems that could impact NS/EP, partnering with the private sector and other critical stakeholders as appropriate.

  - The Government should drive and/or support research to achieve greater clarity around the impacts of hardware-based innovations enabled by new meta-materials and materials science advances, partnering with the private sector and other critical stakeholders as appropriate. The Government should also identify NS/EP risks brought about by the advent of very small sensors, computers, and communications devices or resulting from new capabilities that may be embedded in low-cost, multispectral/hyperspectral sensors.

- **Prepare for the Impact of Quantum Computing, Including its Impact on National Security Information.**

  - The Government should ensure that it is funding and managing the promulgation of quantum-related research and technologies consistent with risk while also contemplating the impact of quantum computing capabilities in the hands of another nation state or a private sector entity. In particular, the Government should review current research and development (R&D) efforts across the ecosystem, taking into account significant efforts underway in the private sector, and determine whether its own R&D efforts are adequately resourced and coordinated. If the Government determines that investment levels need to be increased to support U.S. R&D leadership, then significant engagement with Congress should be pursued. In addition, the Government should consider appropriate controls on precursor technologies for quantum computing, including controls on extreme refrigerants.

  - The Government should focus on the deployment of quantum-resistant encryption and ensure that critical national security information and systems (that will need to remain classified over an extended period of time) are being sufficiently prioritized. In particular, the Government should develop a plan to implement quantum-resistant encryption schemes in a prioritized way, recognizing that deployment may be delayed if cryptographic agility is not sufficiently integrated into relevant technology systems. The Government should also consider the early deployment of hybrid cryptosystems that would combine a new quantum-resistant scheme with an existing, well-studied public-key algorithm, taking into account

the lifetime of sensitive information that is currently being generated and that could be recorded and stored for later decryption.

Cross-Technology Imperatives:

- **Establish a Cybersecurity Moonshot Strategy to Fundamentally Transform the Security of our Digital Landscape within a Decade.**

    - The Government should establish cybersecurity as a national strategic imperative, harnessing the collective resources and capabilities of the Government, private industry, and academic community to simplify cybersecurity consumption and delivery models through accelerated research and action in at least four key and interrelated areas: network design, machine learning, automatic orchestration, and quantum computing. In doing so, the Government should recognize the unprecedented but narrow opportunity for change enabled by disruptive forthcoming technological developments. The Government should also drive accountability for leading the development and implementation of this strategy by designating a senior Government official to lead this cross-Government effort.

- **Institute and Integrate Planning and Preparation for Technology Changes and Landscape Shifts into Existing Cross-Government Efforts.**

    - The Government should institute periodic assessments of disruptive ICT developments by integrating emerging technology-focused scenarios into existing planning exercises, recognizing the pace of ICT developments and the value of regularly considering how the forthcoming environment may shift opportunities and risks. The Government should integrate such future-focused scenarios and planning into existing cross-governmental efforts, such as the Federal Emergency Management Agency's National Level Exercises or the *National Infrastructure Protection Plan*.

    - The Government should foster cross-agency collaboration on technology adoption to lower costs and improve efficiencies and effectiveness by: (1) documenting approaches that address practical scenarios relevant across agencies; and (2) continuing to promote existing incubation efforts and to support technical evaluation labs that help to integrate innovations within functional settings. Examples include programs that promote cross-vendor interoperability at the National Institute of Standards and Technology and that are based on industry partnerships at the National Cybersecurity Center of Excellence.

- **Review Existing NS/EP Public-Private Partnerships to Assess Whether Relevant Stakeholders Are Identified and, to the Extent Warranted, Represented.**

    - 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.[200] 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.

[200] NSTAC. *NSTAC Report to the President on Information and Communications Technology Mobilization.* November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

APPENDIX A: MEMBERSHIP

SUBCOMMITTEE MEMBERS

Mr. Scott Charney, Microsoft Corporation and Subcommittee Co-Chair
Mr. John Stratton, Verizon Communications Inc. and Subcommittee Co-Chair

Ms. Amanda Craig Deckard, Microsoft Corporation and Working Group Co-Chair
Mr. Michael Woods, Verizon Communications Inc. and Working Group Co-Chair

Akamai Technologies, Incorporated	Mr. Thomas Ruff
AT&T Services, Inc.	Mr. Christopher Boyer
Avaya, Incorporated	Ms. Lorraine Cleary
BitVoyant	Mr. Michael Spencer
CenturyLink, Incorporated	Ms. Kathryn Condello
Communications Technologies, Incorporated	Mr. Milan Vlajnic
CSRA, Incorporated	Mr. Guy Copeland
Diogenes Group LLC	Mr. William Gravell
Ericsson, S.A.	Mr. Stephen Hayes Ms. Louise Tucker
Harris Corporation	Mr. Frank Goergen Mr. Michael Troutman
Intel Corporation	Mr. Patrick Flynn Mr. Kent Landfield Mr. Alan Ross Mr. Brian Willis

Microsoft Corporation	Mr. Chris Krebs Ms. Angela McKay
National Institute of Standards and Technology	Mr. Adam Sedgewick
National Security Agency	Ms. Cheri Caddy
Neustar, Incorporated	Ms. Terri Claffey Mr. Rodney Joffe
Palo Alto Networks, Incorporated	Mr. Rick Howard Mr. Sean Morgan
Raytheon Company	Mr. Michael Daly Mr. Brett Scarborough
Sonus Networks, Incorporated	Mr. Kevin Riley
TE Connectivity, Limited	Mr. Todd Bearman
Unisys Corporation	Mr. Mark Cohn Mr. Tom Patterson
Verizon Communications Inc.	Mr. Sanjay Udani

BRIEFERS – SUBJECT MATTER EXPERTS

ATA, LLC	Mr. John Eberhardt, III
AT&T Services, Inc.	Ms. Rita Marty
Avaya Networking	Mr. Paul Unbehagen
Booz Allen Hamilton, Incorporated	Mr. Gary Barnabo Ms. Alexandra Heckler
Center for Strategic and International Studies	Mr. Paul Aughenbaugh
D-Wave International	Mr. Robert Ewald
Dun and Bradstreet Corporation	Dr. Anthony Scriffgnano
General Electric Company	Mr. Richard Puckett
Harvard University/ Resilient Systems	Mr. Bruce Schneier
Hitachi, Limited	Mr. Rich Rogers
IBM Global Business Services	Mr. Daniel Chenok
Intel Corporation	Mr. Steve Grobman Mr. Michael Reed
Intelligence Advanced Research Project Agency	Mr. Kerry Long
Massachusetts Institute of Technology	Mr. John Mallery
Microsoft Corporation	Mr. William Buxton Dr. Jie Liu Dr. Evelyne Viegas
National Academies of Sciences, Engineering, and Medicine	Dr. John Eisenberg
National Institute of Standards and Technology	Dr. Charles Romine

Networking and Information Technology Research and Development Program	Dr. Keith Marzullo
Office of the Director of National Intelligence	Dr. Thomas Campbell
Palo Alto Networks, Incorporated	Mr. Rick Howard
Raytheon BBN Technologies	Mr. J.F. Mergen Dr. Thomas Ohki
Texas A&M University	Dr. Robin Murphy
Utilidata, Incorporated	Mr. Scott DePasquale
Venable, LLP	Mr. Ari Schwartz
Visa, Incorporated	Mr. Gyan Prakesh
WIRED Magazine	Mr. Kevin Kelly

SUBCOMMITTEE MANAGEMENT

President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO)	Ms. Helen Jackson
Alternate NSTAC DFOs	Ms. Sandy Benevides Ms. DeShelle Cleghorn
Booz Allen Hamilton	Ms. Laura Karnas
Total Systems Technology Corporation	Mr. Robert Carter Ms. Ellen Pinson

APPENDIX B: ACRONYMS

3D	Three Dimensional
4D	Four Dimensional
4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network
AI	Artificial Intelligence
AR	Augmented Reality
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DOC	Department of Commerce
DOD	Department of Defense
EUROPOL	European Police Office
ETSV	Emerging Technologies Strategic Vision
GENI	Global Environment for Network Innovation
ICT	Information and Communications Technology
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Infrared
IT	Information Technology
ITL	Information Technology Lab
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
NV	Network Virtualization
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
R&D	Research and Development
RAN	Radio Access Network
RFID	Radio Frequency Identification
SaaS	Software as a Service
SDN	Software-Defined Network
SOC	System on a Chip
TLS	Transport Layer Security
UAV	Unmanned Aerial Vehicle
U.S.	United States
V-2-V	Vehicle to Vehicle
VR	Virtual Reality

APPENDIX C: GLOSSARY

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

Additive Manufacturing – Is defined as the process of joining materials to make objects from three-dimensional (3D) model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies such as machining. (An Additive Manufacturing Test Artifact, Shawn Moylan, John Slotwinski, April Cooke, Kevin Jurrens, and M. Alkan Donmez, Journal of Research of the National Institute of Standards and Technology, Volume 119 (2014) http://dx.doi.org/10.6028/jres.119.017)

Algorithm – A prescribed set of steps to solve a problem. (Newton's Telecom Dictionary)

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

Augmented Reality – A type of human-computer interaction that superimposes the natural visual perception of a human user with computer-generated information (i.e., 3D models, annotation, and text). (Augmented Reality to Supplement Work Instructions, Rafael Radkowski, Model-Based Enterprise Summit 2013, nist.gov)

Authentication – The process whereby a user, information source, or simply information proves they are who they claim to be; the process of determining the identity of a user attempting to access a network and/or computer system. (Newton's Telecom Dictionary)

Binary – The way digital computers function because they represent things only as "ON" and "OFF". (Newton's Telecom Dictionary)

Biometrics – The use of measurable biological characteristics, such as fingerprint recognition, voice recognition, and retina and iris scans to provide authentication. (Newton Telecom Dictionary)

Blockchain – A database that lets mutually-distrusting entities agree on the starting state and history of a system, thereby allowing them to agree on the state of the present system. It allows for the decentralization of databases based on a common understanding of the present state of the system. (Introduction to Blockchains, John Kelsey, NIST, 2016)

Botnet – A network of Internet-connected computers that have been infected by a malicious third-party's command-and-control software and are able to be remotely instructed by that third party to perform harmful actions such as launch attacks over the Internet. (Newton's Telecom Dictionary)

Cloud Computing – A model for enabling on-demand network access to a shared pool of configurable information technology capabilities/resources, (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based

services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. Both the user's data and essential security services may reside in and be managed within the network cloud. (Committee on National Security Systems Instruction (CNSSI) 4009, Adapted) (NSTAC Report 2016)

Critical Infrastructure – System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructure can be owned and operated by both the public and private sector. [*Critical Infrastructures Protection Act of 2001*, 42 U.S.C. 5195c(e)] (CNSSI 4009, Adapted)

Cryptology – Also known as cryptography, it is the process of concealing the contents of a message from all except those who know the key. (Newton's Telecom Dictionary)

Cyber Attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (CNSSI 4009)

'Cyber Kill Chain' Model – Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective. (Lockheed Martin Cyber Kill Chain)

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI 4009)

Denial-of-Service Attacks – The prevention of authorized access to resources or the delaying of time-critical operations. Time-critical may be milliseconds or it may be hours, depending upon the service provided. (CNSSI 4009)

Distributed Denial-of-Service Attacks – A denial of service technique that uses numerous hosts to perform the attack and prevents the authorized access to resources or delays time-critical operations. (NIST Glossary of Information Security Terms – NISTIR 7298 – Revision 2)

Firewall – A piece of hardware or software, or hardware and software, that prevents unauthorized people from gaining access to a computer or computer network. (Newton's Telecom Dictionary)

Hypervisor – A computer software/hardware platform that runs several operating systems simultaneously on the same computer. It is also called virtualization. (Newton's Telecom Dictionary)

Information Assurance – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (NIST SP 800-53, CNSSI 4009)

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

Internet of Things – The total interconnected collection of device networks. (Newton's Telecom Dictionary)

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

Interconnectivity – A term used in telecommunications that describes how to interconnect equipment to equipment, and equipment to telecom lines and networks. (Newton's Telecom Dictionary)

Machine-to-Machine (M2M) – Technologies that enable computers, embedded processors, smart sensors, actuators, and mobile devices to communicate with one another, take measurements, and make decisions - often without human intervention. (Machine to Machine Technology in Demand Responsive Commercial Buildings)

Malware – Software created and distributed for malicious purposes, such as invading computer systems in the form of viruses, worms, or other plug-ins and extensions that mask other destructive capabilities. (Newton Telecom Dictionary)

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

Meshed Network – A network where each node has a direct connection to each of the other nodes on the network. Also called a fully connected network. (Newton's Telecom Dictionary)

Moore's Law – According to Dr. Gordon Moore, the law states that technology continually expands at an exponential and measureable rate. For example, Dr. Moore correctly theorized that from 1965 to 1975, the complexity of integrated circuits would grow from 60 to 60,000. Now all technological advances and increases in knowledge that happen exponentially is colloquially called Moore's Law. (Newton's Telecom Dictionary)

Nano Technology – A collection of various types of research where the characteristic dimensions are less than about 1,000 nanometers. (Newton's Telecom Dictionary)

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

definition based on Executive Order (EO) 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012])

Natural Language Processing – A range of computational techniques for analyzing and representing naturally occurring texts at one or more levels of linguistic analysis for the purpose of achieving human-like language processing for a range of tasks or applications. (Dr. Elizabeth Liddy, "Natural Language Processing", Syracuse University, 2001.) (NSTAC Report 2016)

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

Network Virtualization – A means of improving the efficiency of a network and reducing costs. It involves creating multiple virtual partitions on a single piece of hardware. It cuts down on the amount of network hardware required and allows multiple functions to be managed from a single console. (Newton's Telecom Dictionary)

Neuromorphic Computing – Technology that combines computing fields such as machine learning and artificial intelligence with cutting-edge hardware development and materials science, as well as ideas from neuroscience. In its original incarnation, neuromorphic was used to refer to custom devices/chips that included analog components and mimicked biological neural activity. (p. 5 Neuromorphic Computing, Architectures, Models, and Applications, DOE Workshop Report, June 29- July 1, 2016)

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

Public Switched Telephone Network – The worldwide voice telephone network accessible to all those with telephones and access privileges. (Newton's Telecom Dictionary)

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

Radomes – A plastic cover for a microwave antenna. It protects the antenna from inclement weather, but has little effect on the radiation pattern of the antenna. (Newton Telecom Dictionary)

Software as a service (SaaS) – The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST SP 800-145)

Software-Defined Network – A virtual private network. Specifically, it refers to AT&T's Software-Defined Network Service, which was introduced in 1985 for AT&T's largest customers and provided only dedicated access services. (Newton's Telecom Dictionary)

Stack – 1. A set of data storage locations that are accessed in a fixed sequence. 2. The layers of a technology architecture, with each successive layer being built on and supported by the layers below it. (Newton's Telecom Dictionary)

System on a Chip – A silicon integrated circuit that combines generic functions (e.g. microcontrollers, UARTs, memory, FIFOs, and other analog and digital logic functions) with custom design elements to create a device that contains all major elements of a system on one integrated chip. (Newton's Telecom Dictionary)

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

Virtual Reality – A way of enabling people to participate directly in real-time, 3-D environments generated by computers. It involves the user's immersion in, and interaction with, a graphic screen(s). Virtual reality not only seeks to simulate another world but to have the ability to interact with it in real time. (Newton Telecom Dictionary)

APPENDIX D: SUMMARY NS/EP IMPACT CHARTS

The charts below summarize the national security and emergency preparedness (NS/EP) benefits and risks of each technology discussed in this report. The specific technologies are presented according to the four trends used throughout.

Interconnectivity and processing power

Technologies	NS/EP Benefits	NS/EP Risks
SDN/NFV	• Temporary, special-purpose networks could be constructed for emergency response • Key networks could be rebuilt virtually, bypassing destroyed assets, for quick network recovery • Greater virtual redundancy and resource shifting, increasing resilience	• Planning challenges, e.g., identifying critical infrastructure • Response challenges, e.g., assessing the impact of a destroyed physical asset • Security challenges, e.g., control plane, supply chain
IoT	• More data generation to inform analytics, cognition, and autonomy – aiding in impact assessment, first responder resource allocation, evacuation, etc.	• Challenges related to data protection, data integrity, and maintaining cross-border data flows • Scale of attack surface, e.g., botnets
5G	• Other emerging technologies will likely depend on 5G to operate/advance, including VR/AR, autonomous vehicles, IoT	• As a wide range of devices and services, with different security requirements and levels of criticality, will be supported by 5G, there may be challenges related to building new trust models for security and privacy
Wireless mesh networking	• Can be built in the aftermath of an event, increasing response capabilities • Provide an alternative to existing communications infrastructures and increase survivability due to widely distributed infrastructure, increasing resilience	• Widespread connectivity counter to existing cybersecurity best practices • Work on authentication, encryption, and other security measures necessary
Quantum computing	• Ability to decrypt communications and data protected by public key encryption • Leap forward in computation power, enabling analysis of more data in parallel and more complex modeling, simulations, AI	• Inability to safeguard communications and data not protected by quantum-resistant encryption

Analytics, cognition, and autonomy

Technologies	NS/EP Benefits	NS/EP Risks
Near-term AI	• The ability to utilize advanced planning capabilities • The ability to analyze vast amounts of data quickly to direct efforts most efficiently • More precision and more consistency on a faster time scale	• Lack of algorithmic transparency, accelerated human bias • Security challenges, e.g., manipulation of algorithms • Dependency on apps; lack of coordination with officials
Natural language processing	• Bridging gaps in human-human, human-AI, and machine-to-machine communications • Distinguishing conversations of interest and detecting relationships between entities of interest	• Lack of algorithmic transparency, accelerated human bias • Security challenges, e.g., manipulation of algorithms
Long-term AI	• Range of assistance from intelligent, autonomous units during emergencies, potentially including human-like capabilities, specialist support, and/or context-specific support • Advancements in preparing, planning, integrating experiences and lessons learned	• Lack of algorithmic transparency, accelerated human bias • Security challenges, e.g., manipulation of algorithms • Major economic shifts and governance issues, including NS/EP workforce and regulatory challenges
Autonomous vehicles (land)	• Increased access in disaster response areas • Data from sensors in autonomous vehicles to increase situational awareness	• Privacy challenges with public-private data exchanges • Liability and security challenges • Risk of misuse by malicious actors (e.g., to cause accidents with other land vehicles or entities)
Autonomous vehicles (air)	• Increased visibility of disaster zones, pre- and post disasters, at reduced operational costs • Delivery of communications capabilities	• Data privacy and integrity challenges • Risk of data interception and misuse by malicious actors (e.g., to attack physical infrastructures)

Production and simulation

Technologies	NS/EP Benefits	NS/EP Risks
Ubiquitous (smart) screens	• Greater access to shared resources and opportunities for information sharing and/or immediate cross-referencing to ensure responders have most relevant information • Personalized screens could share personalized information in disaster response	• Data security/privacy and data integrity challenges • Reliability issues • Authentication issues
VR/AR	• Realistic training • Ability to improve situational awareness, e.g., to detect obscured metal • Ability to direct/route people in a more immediate, interactive way	• Lack of availability and dependency (e.g., lack of ability to operate effectively without AR) • Integrity challenges, e.g., risk of manipulation
3D printing	• Ability to quickly develop and deploy a range of specialized products • Simplified supply chain	• Lack of operational expertise • Lack of standards for materials or processes
4D printing	• Ability to quickly develop and deploy specialized products that change form in different environments • Simplified supply chain	• The altering or unexpected emergence of a weapon
Advanced materials	• More devices and connectivity to support greater analytics, cognition, and autonomy • Increased sensory capabilities (visual, auditory, olfactory) • Low weight, high strength materials	• The use of embedded or microscopic devices not visible to the human eye • The unexpected use of sensory amplifications (e.g., to see through walls, hear auditory frequencies beyond natural human range)

Trust and verification

Technologies	NS/EP Benefits	NS/EP Risks
Cybersecurity platforms	• Integration of security technologies to simplify and automate defense, better protecting networks and data • Potential to address workforce challenges by automating processes that have historically required inefficient human intervention	• Potential consolidation of risk exposure
Cybersecurity information sharing	• Increased visibility into security threats and actions to mitigate their impact	• Loss of information to adversaries, enabling them to change tactics or circumvent mitigations
Biometrics	• Improved authentication and authorization to support use of technology with increased confidence • Improved identification methods for national security purposes and emergency responders	• Data security/privacy challenges • Data integrity challenges
Blockchain	• Increased confidence in data integrity • Sharing of information (e.g., cybersecurity threat information) in a trusted way • Widespread digital identity systems	• Widespread dependency • Post quantum, the integrity of blockchain ledgers may be at risk
Quantum-resistant encryption	• Ability to protect communications and data from decryption	• Lack of visibility into communications and data protected by post-quantum encryption

APPENDIX E: BIBLIOGRAPHY

Aaronson, Scott. "Shor, I'll Do It." February 24, 2007. http://www.scottaaronson.com/blog/?p=208.

Abrams, Michael. "Top 6 Innovations in 3D Printing." February 2016. https://www.asme.org/engineering-topics/articles/manufacturing-design/top-6-innovations-3d-printing.

Alejandro Alba. "Augmented And Virtual Reality Might Be Everywhere In 2017." January 3, 2017. http://www.vocativ.com/387662/augmented-virtual-reality-2017/.

Aru, Iyke. "Estonian Government Adopts Blockchain to Secure 1 Mln Health Records." March 9, 2016. https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records.

Aughenbaugh, Scott. Center for Strategic and International Studies. *Briefing to the President's National Security Advisory Committee (NSTAC) Emerging Technologies Strategic Vision (ETSV) Subcommittee.* October 11, 2016.

Ball, Philip. "Quantum Computer Simulates Hydrogen Molecule." July 25, 2016. https://www.chemistryworld.com/news/quantum-computer-simulates-hydrogen-molecule/1010041.article.

Barnabo, Gary and Alexandra Heckler. Booz Allen Hamilton, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* August 16, 2016.

Baraniuk, Chris. "Earthquake Artificial Intelligence Knows Where Damage Is Worst." September 30, 2015. https://www.newscientist.com/article/mg22830412-800-earthquake-artificial-intelligence-knows-where-damage-is-worst/.

Broersma, Matthew. "Mesh Network: The Next Step for Wireless." April 5, 2004. http://www.zdnet.com/article/mesh-networking-the-next-step-for-wireless/.

Brydon, Alastair. "Opportunities and Threats from LTE Device-to-Device (D2D) Communication." February 28, 2014. http://www.unwiredinsight.com/2014/lte-d2d.

Brynjolfsson, Erik and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (2014).

Buxton, William, Jie Liu and Evelyne Viegas. Microsoft Corporation. *Briefing to the NSTAC ETSV Subcommittee.* July 26, 2016.

Campbell, Thomas. Office of Directorate of National Intelligence. *Briefing to the NSTAC ETSV Subcommittee.* June 14, 2016.

Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II.* June 2014. https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Center for Strategic and International Studies. *From Awareness to Action: A Cybersecurity Agenda for the 45th President.* January 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Cheng, Robert. "Not Just Speed: 7 Incredible Things You Can Do With 5G." March 2, 2017. https://www.cnet.com/news/5g-not-just-speed-fifth-generation-wireless-tech-lets-you-do-vr-self-driving-cars-drones-remote/.

Chenok, Daniel. IBM Global Business Services. *Briefing to the NSTAC ETSV Subcommittee.* January 17, 2017.

Conner-Simmons, Adam. "System Predicts 85 Percent of Cyber-Attack Using Input from Human Experts." http://www.csail.mit.edu/System_predicts_85_percent_of_cyber_attacks_using_input_from_human_experts%20.

Crypto Forum Research Group. *Draft: Hash-Based Signatures*. September 6, 2017. https://www.ietf.org/id/draft-mcgrew-hash-sigs-06.txt.

De Filippi, Primavera. "It's Time to Take Mesh Networks Seriously (And Not Just for the Reasons You Think)." January 2, 2015. https://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/.

Deloitte. *Wireless Connectivity Fuels Industry Growth and Innovation in Energy, Health, Public Safety, and Transportation.* January 2017. http://www.ctia.org/docs/default-source/default-document-library/deloitte_20170119.pdf.

Department of Justice. "Declassification frequently asked questions." September 13, 2016. https://www.justice.gov/open/declassification/declassification-faq.

DePasquale, Scott. Utilidata, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* August 2, 2016.

Diamandis, Peter. "Massive Disruption Is Coming With Quantum Computing." October 10, 2016. https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/.

Dowd, Maureen. "Elon Musk's Billion-Dollar Crusade to Stop the AI Apocalypse." April 2017. http://www.vanityfair.com/news/2017/03/elon-musk-billion-dollar-crusade-to-stop-ai-space-x.

Eberhardt, III, John. ATA, LLC. *Briefing to the NSTAC ETSV Subcommittee.* October 25, 2016.

Eisenberg, Jon. National Academies of Sciences, Engineering, and Medicine. *Briefing to the NSTAC ETSV Subcommittee.* July 19, 2016.

EKU Online. "When Disaster Strikes: Technology's Role in Disaster Aid Relief." http://safetymanagement.eku.edu/resources/infographics/when-disaster-strikes-technologys-role-in-disaster-aid-relief/.

Ericsson. *5G Security*. June 2015. https://www.ericsson.com/assets/local/narratives/industries/public-safety/wp-5g-security.pdf.

Europol. "No More Ransom: Law Enforcement and IT Security Companies Join Forces to Fight Ransomware." July 25, 2016. https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware.

Ewald, Robert. D-Wave International. *Briefing to the NSTAC ETSV Subcommittee.* November 1, 2016.

Executive Office of the President (EOP). *Artificial Intelligence, Automation and the Economy.* December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/EMBARGOED%20AI%20Economy%20Report.pdf.

EOP. *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*. April 2011. https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf.

EOP NSTC Council Committee on Technology. *Preparing for the Future of Artificial Intelligence*. October 2016. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

Federal Risk and Authorization Management Program. "About Us." Accessed on: April 10, 2017. https://www.fedramp.gov/about-us/about/.

Financial Tribune. "Cybercrime Cost Global Economy $450 Billion." February 9, 2017. https://financialtribune.com/articles/world-economy/59201/cybercrime-cost-global-economy-450-billion.

Floorwalker, Michael. "10 Innovative Applications for Virtual Reality." September 16, 2016. http://listverse.com/2016/09/16/10-innovative-applications-for-virtual-reality/.

Future of Life Institute. "Autonomous Weapons: An Open Letter from AI & Robotics Researchers." July 28, 2015. https://futureoflife.org/open-letter-autonomous-weapons.

Gartner, Incorporated. "Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage." August 16, 2016. https://www.gartner.com/newsroom/id/3412017.

Geissbauer, Reinhard, Dr. Jorge Lehr, and Mr. Jens Wunderlin. The Future of Spare Parts Is 3D. January 20, 2017. https://www.strategyand.pwc.com/media/file/The-future-of-spare-parts-is-3D.pdf.

Global Environment for Network Innovations (GENI). "What is GENI?" Accessed on: June 19, 2017. http://www.geni.net/.

Goodin, Dan. "NSA preps quantum-resistant algorithms to head off crypto-apocalypse." August 21, 2015. https://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/.

Google. "The New Multiscreen World." https://www.thinkwithgoogle.com/infographics/multi-screen-world-infographic.html.

Government Accountability Office. *Technology Assessment: Internet of Things Status and Implications of an Increasingly Connected World.* May 2017. https://www.gao.gov/assets/690/684590.pdf.

Grobman, Steve. Intel Corporation. *Briefing to the NSTAC ETSV Subcommittee.* March 21, 2017.

Hardawar, Devindra. "Microsoft Has Big Plans for VR and AR in 2017." December 7, 2016. https://www.engadget.com/2016/12/07/microsoft-mixed-vr-holographic/.

Hern, Alex. "Give Robots 'Personhood' Status, EU Committee Argues." January 12, 2017. https://www.theguardian.com/technology/2017/jan/12/give-robots-personhood-status-eu-committee-argues.

Howard, Rick. Palo Alto Networks, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* January 10, 2017.

IBM. "What is Quantum Computing?" Accessed on: June 21, 2017. http://research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

IBM Knowledge Base. "Comparison of IPV4 and IPV6." Accessed on April 7, 2017. https://www.ibm.com/support/knowledgecenter/ssw_i5_54/rzai2/rzai2compipv4ipv6.htm#rzai2compipv4ipv6__compaddress.

Internet Engineering Task Force. *Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms.* November 2015. https://tools.ietf.org/html/rfc7696.

Institute for Soldier Nanotechnologies. Accessed on: July 5, 2017. http://isnweb.mit.edu/soldier-medicine-prevention.html.

Institute for Soldier Nanotechnologies. Accessed on: July 5, 2017. http://isnweb.mit.edu/blast-and-ballistic-threats-materials.html#.

Institute for Soldier Nanotechnologies. Accessed on: July 5, 2017. http://isnweb.mit.edu/lightweight,-multifunctional-nanostructured-materials.html.

The Japan Times. "Mizuho introduces SoftBank's Pepper robot to Tokyo bank branch." July 17, 2015. http://www.japantimes.co.jp/news/2015/07/17/business/tech/mizuho-introduces-softbanks-pepper-robot-tokyo-bank-branch/#.WPE5D_nyvIV.

Jha, Manya. "5 Innovations in 3D Printing." July 18, 2016. https://www.entrepreneur.com/article/279243.

Jones, Brad. "Quantum Computing Will Make You Look Like a Graphing Calculator." September 19, 2016. http://www.digitaltrends.com/features/dt10-quantum-computing-will-make-your-pc-look-like-a-graphing-calculator/.

Kazansky, Becky. "In Red Hook, Mesh Networks Connects Sandy Survivors Still Without Power." November 12, 2012. http://techpresident.com/news/23127/red-hook-mesh-network-connects-sandy-survivors-still-without-power.

Kelly, Kevin. *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (2016).

Kelly, Kevin. Wired. *Briefing to the NSTAC ETSV Subcommittee.* August 2, 2016.

Klein, Alice. "4D Printing Makes Objects That Assemble Themselves When Heated." April 12, 2017. https://www.newscientist.com/article/2127713-4d-printing-makes-objects-that-assemble-themselves-when-heated/.

Kobie, Nicole. "The Quantum Clock Is Ticking on Encryption – and Your Data Is Under Threat." October 4, 2016. http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption.

Kundra, Vivek. Federal Cloud Computing Strategy. February 8, 2011. https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

Lewis-Krauss, Gideon. "The Great AI Awakening." December 14, 2016. https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html?_r=2.

Linn, Allison. "Historic Achievement: Microsoft Researchers Reach Human Parity in Conversational Speech Recognition." October 18, 2016. https://blogs.microsoft.com/next/2016/10/18/historic-achievement-microsoft-researchers-reach-human-parity-conversational-speech-recognition/#sm.0000t2h5i97yof7sqc02rp17ws9iz.

Liquid Newsroom. "Storytelling Everywhere: Everything Can be a Screen." http://liquidnewsroom.com/#product.

Long, Kerry. Intelligence Advanced Research Project Agency. *Briefing to the NSTAC ETSV Subcommittee.* November 15, 2016.

Mallery, John. Massachusetts Institute of Technology. *Briefing to the NSTAC ETSV Subcommittee.* July 12, 2016.

Marr, Bernard. "What is the Difference Between Deep Learning, Machine Learning and AI?" December 8, 2016. https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#4517ab7026cf.

Marty, Rita. AT&T, Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* September 20, 2016.

Marzullo, Keith. Networking and Information Technology Research and Development Program. *Briefing to the NSTAC ETSV Subcommittee.* July 26, 2016.

Mather, Jonathan. "The Energy Blockchain – Believe The Hype, Just Don't Forget The Physics." February 22, 2017. http://berc.berkeley.edu/energy-blockchain-believe-hype-just-dont-forget-physics/.

McGrath, Rita. *The Pace of Technology Adoption is Speeding Up*. Harvard Business Review. November 25, 2013. https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up.

Merel, Tim. "The Reality of VR/AR Growth." January 11, 2017. https://techcrunch.com/2017/01/11/the-reality-of-vrar-growth/.

Merghen, John. Raytheon BBN Technologies. *Briefing to the NSTAC ETSV Subcommittee.* May 24, 2016.

Metz, Cady. "In A Huge Breakthrough, Google's AI Beats a Top Player at the Game of Go." January 27, 2016. https://www.wired.com/2016/01/in-a-huge-breakthrough-googles-ai-beats-a-top-player-at-the-game-of-go/.

Microsoft Digital Crimes Unit. "Digital Crimes Unit uses Microsoft data analytics stack to catch cybercriminals." March 2015. https://msdn.microsoft.com/en-us/library/dn949260.aspx

Moody, Dustin. *Update on the NIST Post-Quantum Cryptography Project.* June 2016. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2016-06/2_post-quantum_dmoody.pdf.

Murphy, Robin. Texas A&M University. *Briefing to the NSTAC ETSV Subcommittee.* August 30, 2016.

Nakamoto, Satoshi. "Bitcoin: A Peer to Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.

Newman, Lily Hay. "The Botnet that Broke the Internet Isn't Going Away." December 9, 2016. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

National Institute of Standards and Technology (NIST). *Report on Post-Quantum Cryptography*. February 2016. http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

National Science Foundation. "Global Environment for Networking Innovations (GENI)." Accessed on: June 19, 2017. https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=501055.

NIST. *Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy*. December 1, 2016. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

NIST. *DRAFT NIST SP800-63A Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*. Accessed on: June 21, 2017. https://pages.nist.gov/800-63-3/sp800-63a.html. See table 5-3 on identity verification methods.

NIST. *NISTIR 8074: NIST's Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*. December 2015. http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf.

NIST. "Announcing Request for Nominations for Public-Key Post-Quantum Crypotgraphic Algorithms." December 20, 2016. https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms.

NIST. "Quantum Computers May Have Higher 'Speed Limits' Than Thought." March 24, 2017. https://www.nist.gov/news-events/news/2017/03/quantum-computers-may-have-higher-speed-limits-thought.

NIST. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf

The National Nanotechnology Initiative. http://www.nano.gov/centers-networks.

National Telecommunications & Information Association (NTIA). "Internet of Things." https://www.ntia.doc.gov/category/internet-things.

NTIA. "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching." https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

NTIA. *Fostering the Advancement of the Internet of Things.* January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

NSTAC. NSTAC Emerging Technologies Strategic Vision (ETSV) Letter to the President. March 10, 2016. https://www.dhs.gov/sites/default/files/publications/Att%20%201%20-

%20NSTAC%20Emerging%20Technologies%20Strategic%20Vision%20%28ETSV%29%20Letter.pdf.

NSTAC. *NSTAC Report to the President on Big Data Analytics.* May 11, 2016. https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Big%20Data%20Analytics%20%284-22-16%29%20%282%29.pdf.

NSTAC. *NSTAC Report to the President on Cloud Computing.* May 15, 2012. https://www.dhs.gov/sites/default/files/publications/2012-05-15-NSTAC-Cloud-Computing.pdf.

NSTAC. *NSTAC Report to the President on Identity Management Strategy*. May 21, 2009. https://www.dhs.gov/sites/default/files/publications/NSTAC%20IDTF%20Report.pdf.

NSTAC. *NSTAC Report to the President on Information and Communications Technology Mobilization.* November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

NSTAC. *NSTAC Report to the President on the Internet of Things.* November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

One Concern. Accessed on April 14, 2017. http://www.oneconcern.com/

Ohki, Thomas. Raytheon BBN Technologies. *Briefing to the NSTAC ETSV Subcommittee.* November 8, 2016.

Partnership on AI. https://www.partnershiponai.org/#.

Prakesh, Gyan. Visa Incorporated. *Briefing to the NSTAC ETSV Subcommittee.* February 7, 2017.

Puckett, Richard. General Electric Company. *Briefing to the NSTAC ETSV Subcommittee.* May 31, 2016.

Ravindranath, Mohana. "Alexa, Can You Tell Me About GSA's Virtual Assistant Pilot?" March 24, 2017. http://www.nextgov.com/emerging-tech/2017/03/alexa-can-you-tell-me-about-gsas-virtual-assistant-pilot/136457/?oref=site-nextgov-flyin-sailthru.

Rogers, Rich. Hitachi, Limited. *Briefing to the NSTAC ETSV Subcommittee.* August 23, 2016.

Reed, Michael. Intel Corporation. *Briefing to the NSTAC ETSV Subcommittee.* February 7, 2017.

Romine, Charles. NIST. *Briefing to the NSTAC's ETSV Subcommittee.* June 28, 2016.

Ross, Alec. *The Industries of the Future* (2016).

Roundtable, Department of Energy, Office of Science. "Neuromorphic Computing: From Materials to Systems Architecture." October 29-30, 2015. https://science.energy.gov/~/media/bes/pdf/reports/2016/NCFMtSA_rpt.pdf.

Rouse, Margaret. "Software Defined Networking (SDN)." August 2015. http://searchsdn.techtarget.com/definition/software-defined-networking-SDN).

Rouse, Margaret. "Network Function Virtualizations (NFV)." March 2016. http://searchsdn.techtarget.com/definition/network-functions-virtualization-NFV).

Ruubel, Martin. "Blockchain-Enabled Cloud: Estonian Government selects Ericsson, Apcera and Guardtime." August 28, 2016. https://guardtime.com/blog/blockchain-enabled-cloud-estonian-government-selects-ericsson-apcera-and-guardtime.

Schneier, Bruce. Harvard University/Resilient Systems. *Briefing to the NSTAC ETSV Subcommittee.* November 8, 2016.

Schwartz, Ari. Venable, LLC. *Briefing to the NSTAC ETSV Subcommittee.* August 27, 2016.

Scriffignano, Anthony. Dun and Bradstreet Corporation. *Briefing to the NSTAC ETSV Subcommittee.* October 18, 2016.

Simonite, Tom. "Build Your Own Internet with Mobiles Mesh Networking." July 9, 2013. https://www.technologyreview.com/s/516571/build-your-own-internet-with-mobile-mesh-networking/.

Simonite, Tom. "One Startup's Vision to Reinvent the Web for Better Privacy." January 13, 2017. https://www.technologyreview.com/s/603352/one-startups-vision-to-reinvent-the-web-for-better-privacy/.

Tobe, Frank. *"How is Pepper, SoftBank's Emotional Robot, Doing?"* The Robot Report. May 27, 2016. https://www.therobotreport.com/news/how-is-the-emotional-robot-pepper-doing.

Turner, Jay. "Responding to Disaster with IoT and SDN mesh." December 23, 2016. https://techcrunch.com/2016/12/23/responding-to-disaster-with-iot-and-sdn-mesh/.

Unbehagen, Paul. Avaya Networking. *Briefing to the NSTAC ETSV Subcommittee.* October 4, 2016.

VanRoekel, Steven. *Security Authorization of Information Systems in Cloud Computing Environments* [Memorandum]. December 8, 2011. https://www.fismacenter.com/fedrampmemo.pdf.

Vehicular Ad-Hoc Network. "Security and Privacy in Location-based MANETs/VANETs." Accessed on April 10, 2017. http://www.ics.uci.edu/~keldefra/manet.htm.

The White House. "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

World Federation of Engineering Organizations. "Engineering for Change." http://www.wfeo.org/next-generation-technology-disaster-preparedness-relief/.

Yu, Alan. "How One App Might Be a Step Toward Internet Everywhere." April 7, 2014. http://www.npr.org/sections/alltechconsidered/2014/04/07/298925565/how-one-app-might-be-a-step-toward-internet-everywhere.

Yurcan, Bryan. "How Blockchain Fits Into the Future of Digital Identity." April 8, 2016. https://www.americanbanker.com/news/how-blockchain-fits-into-the-future-of-digital-identity.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu