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 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 physical and virtual environments. Methods of trust and verification will both increase real-time visibility across the ecosystem and be distributed.

Recent, and forthcoming, innovations and changes have been and will continue to be interrelated, increasing the importance of understanding technology dependencies and deployment timelines. Specifically, some technology 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 (such as 5G) is limited, the deployment of advanced virtual or augmented reality technologies will stall.

Within each area of forthcoming innovation, there are both near- and longer-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 today's language cannot fully describe, 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 this unprecedented growth and transformation in the technology ecosystem, both in the near and longer term? What opportunities and risks should the Government assess in determining whether and how to invest in, prepare for, and deploy various emerging technologies? And how can the Government ensure that the impacts of these technology developments on the Government's existing national security and emergency preparedness (NS/EP) functions are both well understood and appropriately addressed?

The purpose of this NSTAC report is to provide helpful 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; both the Government and the private sector face a range of daunting cybersecurity challenges, both technical and non-technical. 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, business as usual 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 security models and improvements to operational efficiency and governance. Ultimately, investments in national physical infrastructure must be paralleled or even exceeded by a commitment to defense of the cyber realm, and that commitment must be established amidst and reinforced by the multiple waves of forthcoming innovation.

Technology Overview

The technologies discussed within this report are complex, interdependent, and possess varying degrees of predictability; however, there are several organizing and interrelated trends:

Interconnectivity and Processing Power

Over the last two decades, millions and then 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 have been powered in accordance with Moore's Law,[1] as electronics have become less expensive, more compact, and better performing due to consistent improvement of processors. Meanwhile, connections between an ever-increasing number of devices have been supported by improving wireless technologies (such as 4G), Internet protocol (IP) version 6, and other developments that increase the speed, availability, and bandwidth of network connections.

This trend depicts 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

[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.

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 and meshed networks to add unimaginable amounts of data and ubiquitous connectivity. In the longer term, quantum computing and other advanced computing architectures will emerge and transcend Moore's Law.

These developments could greatly enhance the Government's ability to respond to, and recover from, emergency situations, but a more complex and less predictable ICT architecture means that the Government will need well-integrated, strategic plans. Considering how NS/EP functions are impacted by the new environment will become more difficult but more important since the new architecture controls not just critical information but also critical devices and infrastructures in the physical world. Moreover, the Government's efforts to understand and prepare for the NS/EP implications of quantum computing are critical.

Analytics, Cognition, and Autonomy

More devices, more data, more pooled and shared data across environments, and better connections is just the beginning of the story. It is not just about connecting machines, screens, sensors, and people; machine learning and AI will power 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. There is great opportunity inherent in these developments, and there is also 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, including forms of AI that are being commercialized today, and mid-term developments will lead to advances in medical diagnosis, machine translation that removes foreign language barriers, and semi- to fully-autonomous vehicles. In the longer term, experts expect that more mature forms of sentient or even sapient AI will emerge, although the exact range of capabilities and the degree of intelligence or autonomy that will be embedded in this future AI is the subject of discussion and debate.

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, the Government should also consider international AI use, which may be advancing 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 and the need for employees with radically new job skills.

Production and Simulation

As is often cited, 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 how we produce materials; simulate, analyze, and improve production; and experience and interact in both the real and simulated world. This trend will likely result in lower cost, more efficient, and more iterative development; greater potential for shared resources and more interactive learning; and more flexibility in environmental requirements. Technologies that fit within this trend, including ubiquitous screens, virtual reality and augmented reality (VR/AR), 3D and 4D printing, and active nanotechnology, will emerge and evolve over the near and longer term. They will be advanced and enhanced by technologies described within other trends, including 5G and AI, and as use cases are illuminated.

These technologies may substantially augment various NS/EP functions. 3D printing—a lower cost, more efficient, and more personalized method for production—could be used to meet the materials needs of first responders. In addition, VR/AR technologies could not only help prepare first responders and military personnel for deployment, but could also be used to direct resources during a disaster. Micro devices, enabled by advanced materials science, could have many NS/EP applications. Alternatively, an adversary may disrupt or hijack the use of these technologies or independently use these technologies to operate with greater agility.

Trust and Verification

How we enable trusted communications and verify identities, regardless of the platform or activity, will become increasingly important as ubiquitous connectivity, virtual platforms, and intelligence 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 specifically 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 short 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 evolve defensive tactics and mitigate risks. In addition, there will be an increasing need to have trust across a distributed, ubiquitous, and integrated ICT architecture. As such, there will be

an increased use of biometric information to verify identities, including through mobile and other devices. Over the mid-term, technologies that are especially relevant for decentralized systems, including blockchain, will increase in relevance, and technologies that are responsive to new risks, including quantum-resistant encryption, will also be deployed.

As in the context of other technologies described above, the Government must recognize the NS/EP benefits of these trust and verification technologies, while considering their limitations and the new threats that they may create, including loss or alteration of biometric data and dependence on blockchain technologies. The Government should also recognize the importance of both using and preparing to use advanced security technologies that are responsive to advanced threats. For instance, preparing to deploy technologies such as 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 two headings:

1. "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; and

2. "Strategic opportunities" describe new or ongoing activities or missions that the Government should focus on to enable or prepare for longer-term technology developments.

High Priority Actions:

- **Develop a Strategic SDN/NFV Implementation Plan**. The Government should develop a strategic plan, similar to that developed for cloud computing, for the acquisition and efficient implementation of SDN and NFV in Federal networks, taking advantage of the many benefits of this near-term technology. The plan should include specific cybersecurity and supply chain security provisions tailored to the new technology, as well as a plan to address any potential vulnerabilities in SDN/virtualization control plane technologies. In developing the plan, the Government should also 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.

- **Evolve Existing Federal and Critical Infrastructure Protection Guidance to Incorporate SDN/NFV Developments.**
  - The Department of Homeland Security (DHS) should, in consultation with infrastructure operators, review the existing taxonomy of critical infrastructures and assess the specific effects of SDN/virtualization deployment.
  - DHS should develop operational mechanisms that will allow NS/EP planners to 1) accurately locate key virtual assets in the critical infrastructure and 2) leverage SDN/NFV benefits in response and recovery efforts. An initial step should be to ensure that all critical physical and virtual assets are identified.

- **Prepare for IoT Proliferation.** The Government should:
  - Direct the Office of Management and Budget to require Federal departments and agencies to:
    - Conduct an internal assessment to 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
    - Develop mitigation plans to manage security issues created by current and future IoT deployments within the Government. The plans should recognize that IoT devices and their potential uses will continually evolve, and anticipate elements that cannot be fully secured because of the dynamic nature of the IoT and potential threats.
  - Sustain and, where relevant, strengthen investments in convening and facilitating Government and industry forums addressing IoT opportunities and risks, including by
    - Continuing to support public-private partnerships on IoT being pursued by the Department of Commerce (DOC);[2,3,4] and
    - 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.

- **Facilitate Rapid Deployment of 5G Technology by Streamlining the Regulatory Approval Process.** The deployment of 5G technology, a foundational, near-term technology, will enable many other ongoing innovations, including in IoT and VR/AR technologies. 5G technology may also support critical functions in NS/EP contexts.

[2] NTIA. "Internet of Things." Accessed on: April 4, 2017. https://www.ntia.doc.gov/category/internet-things.
[3] NTIA. "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching." Accessed on: April 4, 2017. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.
[4] NTIA. Fostering the Advancement of the Internet of Things. January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

- **Leverage Shared Infrastructure and Services.**[5] The Government should develop an action plan to 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 Federal Government. Leveraging innovative technologies ensures that the Government is better prepared to benefit from and mitigate the risks of forthcoming technologies that will build on the foundation provided by earlier innovations. In addition to security improvements and cost efficiencies afforded by such action, opportunities in analytics, cognition, and autonomy can be accelerated to support operations across the Government.

- **Modernize Government IT/Cyber Procurement.** The Government should reform its procurement processes to achieve the level of agility demanded by the emerging technology environment. The Government should consider:
  - Establishing a special fund that Federal departments and agencies can easily and quickly use to replace legacy IT systems that pose cybersecurity risks to NS/EP critical systems.[6]
  - Establishing a more agile, mission-driven procurement model, perhaps drawing on the experience of flexible models used by the Department of Defense to support the Special Operations Command and other small domains.
  - Empowering Federal departments and agencies to use existing funding for small-scale testing of new technologies or shared services.
  - Establishing dedicated IT procurement teams knowledgeable about forthcoming technologies and skilled in the new agile processes; making such teams available in a cross-agency environment.
  - Accelerating implementation of small scale pilot programs to test new technologies in real world network conditions.

- **Review Existing NS/EP Public-Private Partnerships to Assess Whether Relevant Stakeholders Are Identified and, to the Extent Warranted, Represented.** As discussed within the NSTAC's *Report to the President on Information and Communication Technology Mobilization*, six key players within the cyber ecosystem include entities responsible for users/devices, the customer edge, access, the core, IP services, and applications/content.[7] Particularly relevant to this report, application and content providers, including social media, messaging applications, and AI applications, are increasingly

[5] CSIS. 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.

[6] 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.

[7] 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.

leveraged in an emergency. The Government should assess the communications infrastructure leveraged in an emergency, including all six key players listed above, 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.

Strategic Opportunities:

- **Institute Identification and Assessment of, as Well as Planning for, Disruptive Technologies and Landscape Shifts.** Phase II of the NSTAC study that resulted in this report was structured as a landscape study of emerging technology. Other ongoing efforts have assessed developments around particular technology areas; however, the value of this report is analyzing and presenting a more holistic view of the forthcoming environment. As acknowledged within this report, the pace of ICT developments is incredibly fast and quickening. To ensure that the Government is prepared to adapt to and benefit from future waves of forthcoming technologies, it should institute a process of periodic assessment of developments across the ICT landscape.

- **Develop Approaches to Better Leverage Sharing of Experience and Promote Cross-Government Adoption of Innovative Technologies, Reducing Redundant Learning and Resource Spending.** The Government should continue to promote existing incubation and technical evaluation labs for the integration of innovations within functional settings and emerging automation environments relevant to Government missions. Examples include the evaluation of biometrics products and development of innovative integration methods that promote open systems interfaces, and cross-vendor interoperability at the National Institute of Standards and Technology, and the programs based on industry partnerships at the National Cybersecurity Center of Excellence. The Government should also document recommended approaches to address practical scenarios shared across agencies.

- **Invest in Government Participation in Global Technology Standards Forums.** As VR/AR, 3D printing, AI, and robotics continue to develop and impact new domains and markets, technology will rapidly evolve and new industries will emerge. While industry-led, consensus-based efforts to develop standards to support interoperability among emerging technologies will be critical, over the mid- to long-term, international standards forums will likely also undertake efforts to standardize both aspects of those technologies as well as enabling technologies. 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, in coordination with industry, to support U.S. innovation and continued economic and technological advancement both domestically and globally.[8]

- **Invest in Education and Training Programs, Bolstering Skills Needed for 21st Century Jobs, and Prepare for Changes in Workforce Demands.**
    - The Government should invest in increased and new education and re-training programs to meet Government workforce needs and to have a broader impact on the technology needs of the national workforce. Special attention should be focused upon programs that address developments in AI and machine-to-machine communication.
    - A common aspect of many of these emerging technologies is their heavy impact on the workforce. For example, automated vehicles will not only displace taxi and bus drivers, and farm workers, but also impact our need for on-street parking, reduce the per capita vehicle needs, and have other effects on labor. The Government should prepare for these disruptions in advance and provide training and job placement services in affected disciplines, starting with the Government workforce to develop model programs.

- **Assess New Governance, Legal and Operational Challenges Resulting from Emerging AI, Autonomous Devices, and Related Markets.** The Government should drive, and/or support, research that addresses the need for greater clarity around the impacts of decision-making by autonomous systems, including not only military but also commercial systems that could impact NS/EP. In doing so, the Government should, as appropriate, partner with the private sector and other critical stakeholders. These efforts will prepare the ecosystem for adoption and use of AI and related technologies.

- **Establish a Cybersecurity Moonshot.** The Government should establish a Cybersecurity Moonshot to fundamentally reset the security of our digital landscape within a decade, recognizing the unprecedented but narrow opportunity for change enabled by the disruptive technological developments detailed throughout this report. This Moonshot strategy would establish cybersecurity as a national strategic imperative, harnessing the collective resources and capabilities of the Government, private industry, and the academic community towards a shared vision of fundamentally simplifying the cybersecurity consumption and delivery model through accelerated research and action in at least four interrelated key areas, including: network design, machine learning, automatic orchestration, and quantum computing.

[8] This recommendation is consistent with 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.

- **Prepare for the Impact of Quantum Computing, Including its Impact on National Security Information.**
    - The Government should review current research and development efforts toward quantum technologies and ensure that these are adequately resourced and coordinated. The review should be holistic and take into account significant research efforts underway in the private sector. If the Government determines that investment levels need to be raised radically to ensure U.S. leadership, then significant engagement with Congress should be pursued to help ensure a steady source of funding into the future.
    - The Government should consider the impact of quantum computing not just on military or intelligence agencies, but also on critical commercial functions. The Government should contemplate both quantum in the hands of another Nation state and quantum in the hands of a private sector entity.
    - The Government should identify critical national security information and systems (that will need to remain classified over an extended period of time), and develop a plan for implementing quantum-resistant encryption schemes, recognizing that deployment may be delayed if cryptographic agility is not sufficiently integrated into relevant technology systems. The Government should also consider 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 could be recorded and stored for later decryption.
    - The Government should consider appropriate controls on precursor technologies for quantum computing, including controls on extreme refrigerants.

- **Prepare for the Impact of Micro-Devices on National Security.** The Government should proactively identify risks to national security brought about by the advent of very small sensors, computers, storage, and communication devices enabled by new meta-materials and material science advances. Such devices could be transported undetected into secure compartmented environments or in and on individuals.

- **Facilitate Cross-Government Efforts to Evaluate NS/EP Applications for and Risks of Blockchain Technology.** The Government may explore the use of blockchain technology for efficiently sharing 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.

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