June 2016

The Innovation Landscape and Government's Future Role

Executive Summary

Throughout its history, the United States has relied on innovation to solve its toughest problems. It continues to do so—addressing issues such as cybersecurity, identity, data analytics, and autonomy.

Innovation also drives the nation's economic growth, provides safety and security to its citizens, and helps address global challenges, such as poverty, healthcare, and sustainable development. While most innovation occurs in the private sector, governments play a significant role in fostering innovation, as an acquirer, operator, and regulator of new technology. The next presidential administration will need a broad understanding of the innovation ecosystem and the support of strong federal leadership to enact a plan that enables our nation to continue to enjoy its predominant position on the competitive world stage.

This document discusses the importance of the government's role in sustaining U.S. innovation, in collaboration with academia and industry, focusing on a number of critical technologies and domains. Our goal for this report is to support private-public deliberations on priorities and policies for the future.

A two-pronged attack is needed in which the federal government diligently works to enhance its capabilities, using existing opportunities, while simultaneously looking forward so that it can be better prepared to more rapidly apply future innovations.

Federal Research and Development (R&D) investments have become a critical component of the nation's innovation ecosystem over the past two decades. As the private sector has focused more on later-stage development and its financial Return on Investments (ROI), the sector has significantly decreased its investments in basic and early-stage applied research. According to the Information Technology & Innovation Foundation, "Private sector firms don't fund basic research because it is high risk—it doesn't readily translate into products in the short term. Firms are simply financially unable to address foundational research problems; research addressing basic and broad research questions lies outside the scope of most private investment." Without federal investments in these research categories, the pipeline of new discoveries that enable later-stage development would dry up.

One of the key themes in the National Science and Technology Council report, Science for the 21st Century, is that the national and international research landscape has fundamentally changed and that the federal government must adjust its focus to lead the United States in the new Science & Technology (S&T) ecosystem. The report provides four findings:

- Science & Technology Are Foundational to the American Way of Life
- Research Is a National Investment
- A Global Reorganization of Research Is Happening
- Universities Are Becoming Central Hubs of the Innovation Ecosystem.

Given the importance of innovation to the nation's future and the role of the federal government within the innovation ecosystem, the next presidential administration will need its own innovation strategy. The strategy should strive to successfully balance multiple aspects, for example:

- Encourage current innovation, while also strengthening the foundation for future innovation.
- Address big-picture issues, while also focusing on specific opportunities that are strategically important.
- Accelerate innovation as much as possible, while also enacting policies that protect and encourage implementation of concepts that haven't yet been imagined.

Innovation rarely occurs in a vacuum but rather builds on the successes and failures of prior work by a variety of researchers. Battelle and *R&D Magazine* projected the 2014 U.S. innovation investment to reach $465 billion (B), which represents 2.8 percent of GDP. Industry remains the predominant source (66 percent) and performer (71 percent) of U.S. R&D, with the federal government a distant second at 26 percent and 12 percent (when including Federally Funded Research and Development Centers [FFRDCs]), respectively. America's research universities serve a dual role in the national innovation ecosystem as they perform 60 percent of the nation's basic research and also train the nation's future innovators.

The six focused landscapes in this report indicate sources of innovation that the federal government can leverage to carry out its public mission in novel ways. These chapters also highlight areas in which the federal government can exert influence to drive innovation. It can do so through direct or indirect funding (i.e., funding research or acting as the "leading edge" acquirer of capability) and through policy, regulation, or standardization.

These analyses do not represent a summation of emerging technologies nor a consensus on the most transformative technologies of the next dozen years. Rather, they represent a collection of sectors and technologies that will require federal leadership in the near term to preserve the nation's security and prosperity in the future.

Critical Infrastructure Security and Resilience

The Critical Infrastructure Security and Resilience (CISR) community is focused on enabling the development of evolutionary and transformative approaches to enhancing the security and resilience of CI systems, whether these systems face threats that are manmade (such as a physical- or cyber-attack) or natural (such as a hurricane or pandemic).

The number of these systems and assets across the country is very large. To get a sense of how large, the 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets estimates that the United States has 300,000 oil and natural gas producing sites, 170,000 public water systems, 120,000 miles of major railroads, 5,800 hospitals, and 104 nuclear power plants.

The wide range of possible threats to Critical Infrastructure (CI) include climate change, aging infrastructure, and acts of terrorism, as well as the increased connectivity and interdependency of our infrastructure. The risk of cyber-attacks continues to grow, due to advanced techniques, multiple potential methods of attack (physical, network, and coordinated), and the enormous, enduring impacts of a successful system intrusion, which are transforming cyber-physical systems (CPS) attacks into low-risk, low-cost, high-yield endeavors. In addition, business efficiencies and industry consolidation can actually increase the number of single points of failure in CI.

The nation's CI comprises a complex, highly-interconnected and distributed system-of-systems (SoS). While each individual sector protects its own SoS, vulnerabilities exist at the interface(s) between sectors. Thus, the outcome of a CISR strategic approach is a more secure SoS that prevents or withstands attacks, thereby reducing the likelihood and impact of a large-scale disruption of critical services to millions of Americans.

Of critical importance to this CISR strategy is the recognition that the government is not in a position to address all potential CISR vulnerabilities and challenges faced by civilian and defense agencies, as most of the CI in the United States is owned by the private sector. To achieve enduring resilience, the government and the private sector must identify the most critical CISR issues and work together to identify priorities, required resources, strategic partners, and outcomes. Outcomes should include greater cyber-physical security, advanced threat detection and mitigation, and advanced capabilities to respond to and recover from CPS attacks.

A large number of players within the United States are working on various CISR-related topics, including universities, national laboratories, government organizations, and commercial entities. Reflecting the fact that there are CI dependencies at the system, local, regional, and national levels, Sector-Specific Agencies (SSAs) and sector stakeholders undertake R&D activities in CPS security, as appropriate to their unique risk and operating environments. Many CI systems involve CPS and thus offer opportunities to address the increasing autonomy and cooperation possible while providing greater assurances of safety, security, scalability, and reliability.

A number of CISR areas could be addressed to ensure that continual improvements are made across the various sectors. Some of the biggest challenges to achieving CISR, however, are not technological but rather political and economic. For example, local, state, and federal government entities need to develop effective and efficient methods of sharing information to achieve a common operational picture.

Cybersecurity

Cyber-attacks against public and commercial enterprises continue to grow in sophistication. Malware and advanced persistent threat (APT) campaigns not only account for frequent serious data breaches and financial and intellectual property theft, they threaten

national security. A thriving commercial marketplace has emerged to meet the demand for innovative cybersecurity solutions.

The federal government has responded, as well. In 2011, federal research agencies jointly developed "a strategic plan for cybersecurity R&D that confronts underlying and systemic cyberspace vulnerabilities and takes maximum advantage of the federal government's unique capabilities as a supporter and champion of fundamental research."

A new inter-agency team is in the process of updating the 2011 strategy in response to new federal legislation. In addition to this federal strategy, several agencies have created and are maintaining agency-specific strategies for guiding their investments in cybersecurity R&D. The agencies' strategies are well-coordinated via the Cyber Security Inter-Agency Working Group.

The U.S. federal cybersecurity market is valued at $65.5B cumulatively over five years (2015-2020). A key differentiator for companies in the cybersecurity space is access to robust cyber-threat information. For example, companies such as Mandiant are intimately involved in helping companies recover after major APT attacks and have built robust threat intelligence capabilities and databases. Awareness and knowledge of the real threat enables innovators to build cybersecurity capabilities that have impact on adversaries.

Cybersecurity is a continually evolving problem with innumerable challenges to be addressed. There is still a need for strong cybersecurity foundations, especially with the expectation that quantum computing will become a reality within a few decades. At the same time, new challenge areas are emerging as potential priorities, such as cyber deterrence, mission assurance, adaptive security, and CPS security. In addition, some technologies (e.g., identity, authentication, and access management) are being re-examined in light of the increasing momentum and scale of the Internet of Things.

The rapid pace of innovation has prompted the Department of Defense (DoD) and the Department of Homeland Security (DHS) to establish offices in Silicon Valley to develop deep public-private partnerships, both to transition technologies developed by government and national labs, and to leverage technologies developed by industry. Indeed, a whole-of-nation approach is essential to tackling the vast challenges of cybersecurity.

Data Analytics

Data analytics is a broad area—encompassing data science, big data, statistical processing, decision aids, and machine learning—that is focused on providing a "decision advantage" for an organization.

Big data is big news for a reason. The transformational change it has promulgated can be measured by dramatic increases in efficiency (of resource utilization and cost avoidance), effectiveness (of outcomes), timeliness, and/or accuracy of decisions. The value of improved information accuracy and timely situational awareness can be counted in lives saved, costs avoided, or fraud detected.

Numerous technologies support data analytics, from developing data-analysis algorithms to fusing and visualizing complex data so it can be quickly understood and acted on. Data analytics advancements will also rely on a number of critical global and national investments and partnerships among research centers, academia, and industry.

Research centers have been investing for years in a complete approach that includes exploitation of data as well as data presentation and option awareness concepts. Researchers are striving to show users that with the right data they can make better and more timely decisions than if they rely solely on their intuition and experience.

There are various ways to describe and cluster key U.S. investments related to analytics technology investment areas. One is by technology: big data, machine learning, visualization, and decision support. Another is by domain mission area, including intelligent cities, fraud and financial stability, and healthcare. Overall data analytics investment continues to rise and this momentum is projected to continue for the next several years.

In the mid-1990s, the rise of e-mail made the Internet more accessible to consumers and drove user adoption. Similarly, data visualization tools will make data analytics more accessible in coming years. Visual analytics (also called data discovery or data exploration) allows users to ask interactive questions of their prepared data sets and get immediate responses in a visual format that makes the whole process engaging and understandable. This capability will democratize access to data and foster a strong data analysis culture in which business users will look for data and perform visual analyses before making decisions.

There are dangers, however, in the democratization of data. Before government leaders make decisions based on colorful new visualizations, they need to be positive their data is accurate and their tools are built on decision-science principles, which is not a given for today's systems. The majority of people today believe what they read on the Internet, and they are very likely to believe and make decisions based on real-time visualizations that come from drop-down menus in exciting graphic tools. Quick visualizations do not guarantee accurate decision making.

Smartphones and tablets have fundamentally changed consumer habits. Mobile video is the fastest growing segment of mobile data traffic. Organizations need to think strategically about engaging with citizens/consumers on their mobile devices. The top priorities for companies will be defining mobile metrics that matter, understanding mobile technology and the data creation process, and collecting and analyzing mobile data. Challenges include addressing security and privacy concerns.

Other areas to address for the future include adoption of cloud services and predictive analytics. Investing in data analytics systems requires knowledge of how they work, including the long-term costs. Government financial and acquisition policies are not yet in sync with the requirements of building complex learning systems.

Identity

The act of establishing an individual's identity and subsequently using that identity for a range of government and non-government purposes requires a family of technical tasks that have become both increasingly important and increasingly difficult. They occur against a backdrop of accelerating technical opportunities for all actors and a proliferating operational and security challenge for the government.

Identity itself can be established using biometrics (e.g., fingerprints and iris images), registered using unique identifiers or other credentials (e.g., Social Security Numbers, birth certificates, and Common Access Cards), and confirmed through ancillary methods such as interviews, biographical details, and passwords.

At its essence, the problem of identity is the problem of establishing and maintaining a set of facts that, taken together, confirm that a given person is who he says he is, or who we think he is. For any such scheme to work, some of these facts must not be generally known; otherwise, anyone could use a set of correct facts to claim a given identity. Criminals, hostile governments, and malicious non-state actors see high-value in identity data for just this reason and are highly motivated to steal and use it for their various purposes.

The use of innate facts—biometrics—is helpful in identifying a person, but even so, some potential attack vectors via spoofing are known and others may emerge. Established biometrics technologies include palm print recognition, fingerprint recognition, hand geometry, dynamic signature, vascular pattern recognition, iris recognition, face recognition, and speaker recognition. Emerging biometrics technologies include deoxyribonucleic acid (DNA) forensics, tattoo recognition, stand-off iris recognition, all-aspect face recognition, facial aging, behavioral biometrics, and social and demographic signatures.

Choosing authentication strategies to match the practical and policy constraints of a given government or private-sector use case will loom increasingly large in coming years. Developing strategies for authentication and other identity management actions in the face of compromised databases is an emerging challenge that cannot be ignored.

Internet of Things

The Internet of Things (IoT) refers to a decentralized interconnected network of devices (e.g., sensors and actuators), applications, and services that are deployed on a massive scale for sensing, controlling, and interacting with the physical world. Gartner defines the IoT as "a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."

We know that IoT enables operational capabilities and experiences far surpassing anything we have known to date from computer systems. It also presents unprecedented opportunities in the private and public sectors, from efficient management of our physical infrastructure to real-time response to natural or man-made disasters. At the same time, it presents

serious vulnerabilities and operational risks that need to be understood and managed to the extent possible.

There is ongoing private and public R&D activity around many of these security topics, as well as large-scale design and integration challenges. Many universities, for example, have developed capabilities that are directly related to either large-scale IoT research or one of the enabling technologies for IoT.

The IoT will proliferate rapidly over the next few years as networked devices, including sensors, actuators, and a host of smart devices, continue to come online. The IoT will not only have a huge impact on the consumer market, these devices will increasingly be embedded into the nation's critical infrastructure and military systems. This makes it especially important to understand the implications of this particular technological evolution on our social and political fabric, both positive and negative.

The U.S. government will not be the major driving force behind the IoT wave, which is already building faster and higher than most government organizations had expected. Rather, we believe that there is a window of opportunity within which the government can properly study and understand the radical changes and implications that will be wrought by such a massive scale of connectedness across the globe. With a more well-informed approach to IoT, the government will be positioned to benefit from, and properly use, the vast array of capabilities that will emerge. Perhaps more important, however, the government will be in a stronger position to mitigate the risks manifest in IoT.

Trustworthy Autonomy

The DoD defines an autonomous system as one that is able to "make decisions and react without human interaction." In the near future, we are likely to see increasingly autonomous systems helping to diagnose illnesses and determine courses of treatment, make investment decisions for individuals, and analyze large volumes of intelligence data to make conclusions about security risks. Further in the future, we are likely to see autonomous delivery vehicles (in the air and on the ground), driverless taxi-cabs, container ships that unload themselves, aircraft that refuse to crash, mines operated by just a handful of individuals, and combat aircraft that can penetrate air defenses without a pilot onboard.

Today's automation system researchers, designers, and developers are building complex, interconnected, non-deterministic, adaptive systems to improve people's safety, security, and prosperity. Our common vernacular often refers to such systems as "autonomous." Algorithms used in "autonomous" systems tend to be so sophisticated they are not simply measuring the environment with sensor data but *perceiving* what the measurements may mean (often referred to as perception). Decision algorithms go beyond simple heuristics (e.g., if-then) to algorithms that reason and make judgments about the correct course of action.

Increasing autonomy—whether part of a cyber-physical system (e.g., unmanned vehicles, the power grid, medical devices, command and control systems) or part of a purely cyber system (e.g., high frequency trading, medical diagnosis, intelligence analysis)—presents many challenges for the government, which acts as an acquirer, provider, and regulator of these technologies.

While the United States has been the international leader in innovation associated with automation and information technology for many years, other countries are now catching up. For example, Germany, Australia, the United Kingdom, Japan, Israel, China, and India are not only demonstrating technology innovation in the area, they are also quickly putting the technology into operational mode.

Government and industry continue to work on the many challenges surrounding increasingly autonomous systems. This includes the technical challenges of creating algorithms associated with the perception and reasoning capabilities required for operations. In the past, such technology revolutions would not be possible without significant government R&D investment to ensure innovation. As with the Information Technology (IT) revolution, however, the potential for significant ROI means private industry is investing in the R&D that will lead to many, if not most, of the significant innovations expected in the autonomous system area.

Government, however, has a critical role to play in the future of autonomous systems as the objective regulator that will ensure the safety and security of the American public. The United States needs to advance its mechanisms and policies for oversight, testing and evaluation, and certification of autonomous systems. It is especially important to ensure the resiliency of systems that, if they fail or underperform, could trigger dire consequences from a safety, security, or prosperity perspective.

Acknowledgments

Thank you to the following for researching, writing and editing this report:

Duane Blackburn
Jim Cook
Mark Maybury
Rick Sciambi
Beverly Wood
Robert Coury
Rob Case
Rod Holland
Rick Knowles
Andy Lacher
Randall Landry
Nick Orlans
Mindy Rudell
Vipin Swarup

Table of Contents

Innovation:

The process of improving, adapting, or developing a product, system, or service that delivers better results.

Introduction – The Importance of Innovation to Our Nation

> America's future economic growth and international competitiveness depend on our capacity to innovate. We can create the jobs and industries of the future by doing what America does best – investing in the creativity and imagination of our people. To win the future, we must out-innovate, out-educate, and out-build the rest of the world.
>
> —Executive Office of the President, *A Strategy for American Innovation* (2011)

The United States (U.S.) is an innovative nation. The assembly line, air conditioning, personal computers, mobile phones, and microwave ovens—even masking tape and clothespins—were all birthed by American ingenuity. These innovations, and hundreds more, play a significant role in sustaining our nation's economy, security, and way of life.

Innovation "is the foundation of American economic growth and national competitiveness" [1]. The United States has led the world in innovation since World War II; however, our dominance is declining as other countries aggressively work to raise their standing through investments and pro-innovation policies [2]. By many measures, the United States remains the top innovative country, but is no longer dominant. Individual countries, such as China and Japan, are now innovating at roughly the same order of magnitude and may be poised to pass the United States within a decade.

In addition to competition from abroad, the United States faces many internal barriers to innovation. For example, basic research and Science, Technology, Engineering, and Math (STEM) education, the foundational items that serve as the pipeline for future innovation, continue to lag behind policymakers' targets. A review of triadic patent applications, an indicator of mid-term innovation opportunities, shows that the United States has already been passed by the European Union (E.U.) and Japan [3].

In the shorter-term, there are a number of opportunities—as well as coinciding citizen expectations—for applying recent innovations within the federal government. However, government adoption of these innovations is often delayed by administrative and regulatory processes. Laws, government regulation, and policy must keep up with technological advances if both public and private organizations are to gain the benefits these technologies promise. For example, advances in precision medicine could revolutionize the treatment of disease, but they may require changes in both patent law and the new drug approval process to make the pharma business model viable in the face of new technologies. Likewise, advances in identity technologies could be leveraged to allow more secure interaction with the government, but they may require new policy and regulation to enable their use.

One of the key roles for the next presidential administration should be developing and implementing a U.S. innovation strategy. While the "private sector is America's innovation engine," [1] the federal government plays an important role, both directly and indirectly, within the nation's innovation ecosystem. It can drive or leverage innovations to fulfill its mission and provide a foundation that makes future innovation possible.

This document discusses the importance of the government's role in sustaining U.S. innovation, in collaboration with academia and industry, focusing on a number of critical technologies and domains. Our goal for this report is to support private-public deliberations on priorities and policies for the future.

Enhancing the Adoption of Innovation Within Federal Applications

The federal bureaucracy is massive and slow moving. It is predominantly designed to perform reliably, rather than to quickly adjust to changing circumstances. The majority of government leaders, however, acknowledge the need to change both culture and process to take advantage of the rapidly changing innovations available to them. Issues calling for innovation include:

- Government strategies and federal programs are increasingly being directed to enable person-centric services, with agencies unprepared to function in such a manner.
- The populace's expectations for timely communications on a variety of platforms is far outpacing the federal government's communications and archiving infrastructure, which in many cases is still struggling to properly manage email.
- Tightening budgets call for enhanced insights into the Return on Investments (ROI) of numerous areas of government-wide focus, as the government still struggles with determining how much it spends on the topic at a single agency.

By its very nature, however, federal and state governments must operate differently than the private sector so many commercial innovations cannot be directly ported into service. First, government must comply with a stream of operational requirements, regulations, procurement laws, and a complex appropriations process. Changing the status quo will require forward-thinking and energetic leadership at the individual and agency levels, which can be hard to find and nurture within the federal bureaucracy's risk-averse culture.

A two-pronged attack is needed in which the federal government diligently *works to enhance its capabilities*, using existing opportunities, while simultaneously looking forward so that it can be *better prepared to more rapidly apply future innovations*.

Enhancing Capabilities Using Existing Opportunities

This approach takes a significant amount of energy, and there is no "one size fits all" solution. Opportunities must be identified, prioritized, individually examined, and addressed.

Administration– or Department–level leadership must identify and prioritize opportunities and then ignite them into areas of rapid transformation.

One approach to consider is establishing a consortium of members from academia, industry, and government to foster collaboration and advancement on a specific issue, somewhat similar to current efforts at spurring innovation in specific geographical regions. These groups could adopt relevant lessons learned on management from existing regional hubs, as well as similar organizations.

Example Collaborations

The National Cybersecurity Center of Excellence (NCCoE) is a U.S. government organization that builds and publicly shares solutions to cybersecurity problems faced by U.S. businesses. The NCCoE identifies issues that affect major sectors or reach across multiple sectors. It then forms a team of individuals from a variety of technology companies, federal agencies, and academia to solve the problem.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) acknowledges and addresses a major weakness in cyberspace—a lack of confidence and assurance that people, organizations, and businesses are who they say they are online. The Identity Ecosystem Steering Group is a private sector-led organization created to meet NSTIC goals. It consists of a diverse group of stakeholders, including regulated industries and Information Technology (IT) infrastructure developers, consumer advocates, educational organizations, and civil liberties groups.

The federal government also needs to identify and implement methods to overcome its predominantly risk–averse culture so that its employees are energized to drive adoption of innovative approaches rather than being content with the status quo. The Partnership for Public Service and the Hay Group identified four barriers to innovation in government:

- The absence of a process to introduce and grow new ideas
- Gaps in communication and ever–shifting priorities
- Lack of funding to experiment
- A system that rewards the status quo

Its report includes nine attributes of successful innovation leaders within government [4]. Government needs to analyze studies such as this one and develop agency–specific strategies and roadmaps.

> Federal innovation leaders stand out from their private-sector counterparts because of their ability to drive innovation despite complex processes, competing agendas, deep hierarchies and static cultures that can stifle even the most insignificant collaboration and risk-taking – let alone real innovation.
>
> —Hay Group, *Leading Innovation in Government* (2011)

Looking Forward to Enable Future Integration

Adapting existing capabilities can be difficult because doing so often means cramming a square peg into a round hole. Imagine how much easier it would be if the government saw that a square peg was coming and took steps to design a square hole in advance. While it may be impossible to know the exact dimensions of the square hole, government could identify the basic parameters ahead of time and design flexibilities into its systems and approaches so that future integration is much easier, faster, and cheaper to achieve.

The private sector regularly performs *technology forecasting* to predict the future characteristics of useful technologies, procedures, and/or techniques. These studies attempt to "shed light upon the nature, magnitude, probability and timing of relevant scientific and technological developments" [5]. Forecasting exercises help companies strategically position themselves for the environment of the future.

Unfortunately, it is rare for federal entities to practice forecasting. This lack of foresight is a major reason why federal adoption of innovation lags behind the private sector. The government could certainly adopt technology forecasting practices, but this will require Executive Branch leadership and Congressional support. A first step could be to understand both the overall innovation landscape and specific details about critical innovation areas, which are provided in this document.

Subsequent steps will require agency programs to perform targeted technology forecasting exercises. As this is a foreign concept for the majority of those in the federal service, they will require training and roadmaps to understand how to be successful.

The Federal Government Supports Future Innovation

> Undoubtedly the capability to innovate and to bring innovation successfully to market will be a crucial determinant of the global competitiveness of nations over the coming decade. There is growing awareness among policymakers that innovative activity is the main driver of economic progress and well-being as well as a potential factor in meeting global challenges in domains such as the environment and health. Not only has innovation moved to centre-stage in economic policy making, but there is a realisation that a co-ordinated, coherent, "whole-of-government" approach is required.
>
> —OECD in *Innovation and Growth: Rationale for an Innovation Society* (2007)*
>
> *Organisation for Economic Co-Operation and Development. Available: http://www.oecd.org/science/inno/39374789.pdf

Innovation drives a nation's economic growth, provides safety and security to its citizens, and helps address global challenges, such as poverty and sustainable development. While most innovation occurs in the private sector, governments play a significant role in fostering innovation, as an acquirer, operator, and regulator of new technology. The next presidential administration will need a broad understanding of the innovation ecosystem and the support of strong federal leadership to enact a plan that enables our nation to continue to enjoy its predominant position on the competitive world stage.

The U.S. government fosters innovation in three primary ways: (1) *ensuring a well-functioning market*, (2) *targeted innovation programs*, and (3) *supporting innovation's technological pipeline*.

A Well-Functioning Market

Organizations and individuals must be motivated to take calculated risks and engage in entrepreneurial behaviors. Federal assurance of a fair and balanced (i.e., free) market is not only required but can also encourage more innovation and faster adoption of the best ideas. For example, the deregulation of the telecommunications industry in the mid-1980s created competition, which fostered innovation, which led to the introduction of new features such as voicemail, call-waiting, call-forwarding, and touchtone.

The standardization process is another attribute of a well-functioning market. While at first thought "standards" may seem to be contradictory to "innovation," they actually support innovation by providing shared platforms and interfaces. For example, innovative mobile phone apps wouldn't be possible without standards for how apps interact with the phone's processing and display features. Standards can also support innovation by facilitating business interactions, speeding innovative products to market, and providing interoperability among different products and services.

Recognizing the importance of standards, the National Technology Transfer and Advancement Act of 1997 gave the National Institute of Standards and Technology (NIST) the job of coordinating government's development and use of technical standards and aligning these activities with the private sector. The mission of NIST, a non-regulatory federal agency within the U.S. Department of Commerce, "is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life" [6].

The Balancing Act of Intellectual Property

"Innovation often occurs when individuals leverage ideas and capabilities developed by others in new ways. Furthermore, innovation on complex issues often requires collaboration from a variety of parties, including entities that are normally competitors. Both of these examples raise intellectual property (IP) concerns, which can be described with the following analogy: "I think of IP in much the same way that I think of intelligence data. We need to protect it, but it does little good when not shared."

Intellectual property protection must be carefully considered in view of the technology area and the maturity of the respective technologies. While organizations must manage IP disclosure to protect significant investments or to maintain a competitive advantage, it is also the case that the IP that results from pre-competitive research and development can be beneficially shared across communities or organizations to enhance downstream commercial success.

While we must protect IP, we must also shrewdly share it for the benefit of the U.S. economy and the companies who perform such sharing. In many cases, innovation can be enhanced by entering into agreements that clearly delineate IP rights, by disclosing IP up front to enhance the pace of research and avoid subsequent inadvertent or unplanned disclosures, and by having reasonable and non-discriminatory licensing policies."

—Barry Costa, Director of MITRE's Technology Transition Office

The value of innovation to a nation would dramatically suffer without strong intellectual property (IP) rights, such as patents and copyright protections. IP laws and regulations help ensure that the rights to sell newly created innovations reside with the inventors. Without this protection, the incentive for the vast majority of innovation would cease to exist. It is the role of governments to strike the right balance on this front as IP rights that are too broad and/or too restrictive can stifle innovation for an entire technology class.

Targeted Innovation Programs

The federal government often uses targeted incentives to motivate external innovation. For example, creating indirect incentives through the tax system to encourage private companies to invest in Research and Development (R&D) has been a successful, long-term effort. "Governments around the world routinely offer tax incentives to private companies for their R&D spending . . . . Tax incentives reduce the marginal cost of R&D and thus stimulate more of it" [7]. Examples of more direct incentives from the current administration include:

- Hosting challenges and incentive prizes to encourage the private sector to overcome specific government challenges [8].

- The *US Ignite Partnership*, which aims to establish a new foundation for America's broadband future [9].
- *Startup America,* a White House initiative launched to celebrate, inspire, and accelerate high-growth entrepreneurship throughout the nation [10].
- The National Robotics Initiative, whose goal is to accelerate the development and use of robots in the United States that work beside or cooperatively with people [11].
- *Innovation for Global Development*, which commits the United States to accelerate progress in areas such as global health, food security, nutrition, clean energy, and financial inclusion [12].

Supporting Innovation's Technological Pipeline

Of the three ways for government to influence innovation, this arguably has the largest and most sustained impact. Basic and early-stage advanced research, which is predominantly funded by the federal government, increases scientific knowledge and technological capabilities that serve as the foundation for future innovation.

As an example, consider one innovation that has fundamentally changed the daily lives of the majority of Americans over the past decade: the mobile phone. This technology was developed by the private sector to drive future company profits by providing previously unimagined capabilities to its users. The innovation, however, was only made possible by leveraging a host of prior R&D successes funded and managed by the federal government (see Figure 1).

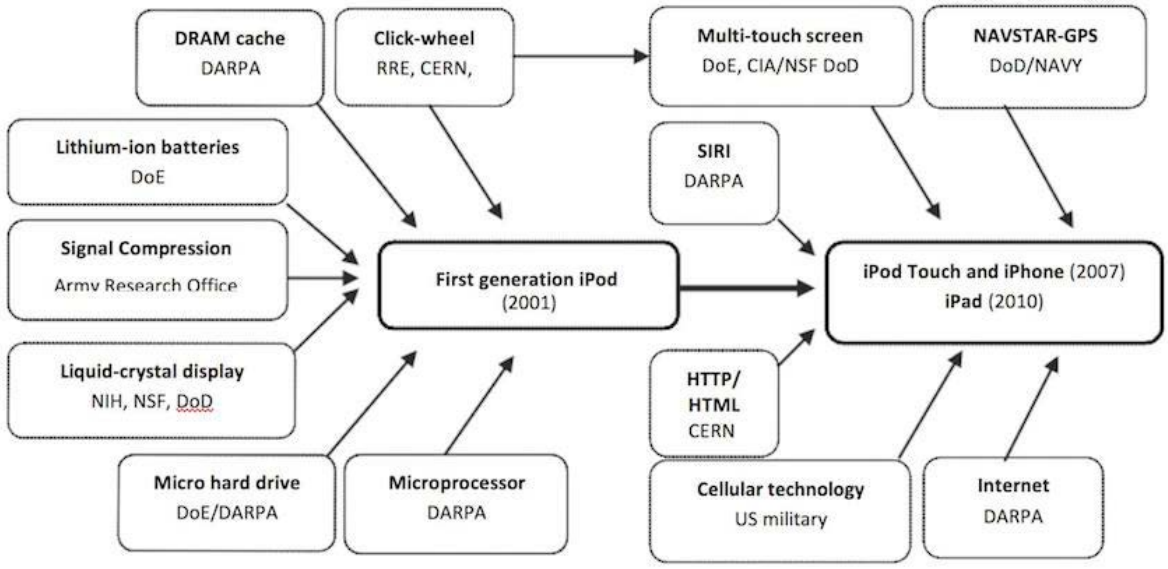

Figure 1. Federal Investments Led to the Creation of the Smartphone [13]

Other recent private-sector innovations made possible by prior federal research include the Internet, GPS, Google's search engine, flat-screen televisions, MRI machines, and lactose-free milk [13].

Federal R&D investments have become a critical component of the nation's innovation ecosystem over the past two decades. As the private sector has focused more on later-stage development and its financial ROI, the sector has significantly decreased its investments in basic and early stage applied research. Private sector firms "don't fund basic research because it is high risk—it doesn't readily translate into products in the short term. Firms are simply financially unable to address foundational research problems; research addressing basic and broad research questions lies outside the scope of most private investment" [13]. Without federal investments in these research categories, the pipeline of new discoveries that enable later-stage development would dry up.

The following section provides a more in-depth look at U.S. Science & Technology (S&T) best practices and challenges, including analyses performed for the Bush and Obama presidential administrations.

Past Federal Studies on the Importance of S&T

Vannevar Bush's seminal report, *Science: the Endless Frontier*, [14] is considered a "constitution" by the U.S. science community [15] in that it identifies principles that the federal government must advance and respect in order for S&T communities to meet the nation's future needs. These principles include the stability of long-term funding, research grants to independent institutions, and pursuit of projects consistent with agency missions.

The science advisors for our two most recent presidents have both commissioned similar analyses to investigate the importance of S&T to the nation's future and the federal government's role within the nation's innovation ecosystem. The two administrations, however, took differing approaches to their investigations: President Bush's science advisor attacked the issue by gathering experts from within the federal government, whereas President Obama's science advisor convened a panel of experts from the private sector.

Science for the 21st Century (2004)

> Through science we generate new knowledge and discovery, become inspired as we coax nature to reveal her myriad secrets, and expand our understanding of the physical and living world. A strong scientific enterprise produces new tools for analysis and investigation and increases our capacity to question, learn, and build on previous accomplishments. Science points us toward innovative solutions to today's major challenges, provides the foundation for economic growth and development, and enhances our quality of life.
>
> —Science for the 21st Century (2004)

Science for the 21st Century [16] is a document produced by the National Science and Technology Council (NSTC) [17], a White House led interagency forum that identifies and prioritizes S&T topics from a whole-of-government perspective. The Council then serves as a mechanism to coordinate and oversee subsequent federal activities.

The document's key theme is that the "Federal Government plays a key role in supporting the country's science infrastructure, a national treasure, and scientific research, an investment in our future." Federal investments in R&D, historically about 28 percent of the nation's overall investment, play a "crucial role in maintaining our nation's preeminence in science." The federal government supports:

- The majority of funding for fundamental research that may have no immediate application.
- Research that requires sustained levels of long-term investment.
- Major research facilities that are beyond the capacity of private industry to build or sustain.
- An infrastructure of measurements and standards that pervade the nation's science and technology base and that are essential to the progress of science and innovation.
- Applied R&D for national priorities combined with partnership efforts that accelerate the transition of federal research results into practical applications.
- Programs for ensuring excellence in our national S&T education and workforce development.

According to this document, the federal S&T enterprise has four major responsibilities, each of which is discussed in depth:

1. Promote discovery and sustain the excellence of the nation's scientific research enterprise.
2. Respond to the nation's challenges with timely, innovative approaches.
3. Invest in and accelerate the transformation of science into national benefits.
4. Achieve excellence in science and technology education and in workforce development.

The document also touches on the ever-present issue of public perception: "Promoting a scientifically educated and aware public is necessary if we are to make the appropriate decisions about the nation's R&D investments, guide the adoption and debate the societal implications of new science and technologies, and reap the maximum benefits from our investments. The quality of these efforts underpins the entire U.S. scientific enterprise."

Transformation and Opportunity: The Future of the U.S. Research Enterprise (2012)

> No country in the history of the world has more readily, or more fruitfully, embraced innovation through science and technology than the United States. The products of our basic and applied scientific research not only provide us with high-quality jobs and support our high-tech and knowledge economies, but they also define us as a nation: We are an inventive, entrepreneurial society.
>
> —Transformation and Opportunity: The Future of the U.S. Research Enterprise (2012)

Transformation and Opportunity: The Future of the U.S. Research Enterprise [18] is a document produced by the President's Council of Advisors on Science and Technology (PCAST) [19], a group of the nation's leading private-sector scientists and engineers. These experts advise President Obama and the Executive Office of the President on many areas in which understanding science, technology, and innovation is key to strengthening our economy and forming policies that work for the American people.

The document's key theme is that the national and international research landscape has fundamentally changed, and that the federal government must adjust its focus to lead the United States in the new S&T ecosystem. It provides four findings that drive a series of opportunities:

- **S&T Are Foundational to the American Way of Life.** "The benefits from scientific advances, and the need for such advances to continue, are evident in virtually every aspect of modern life. We want longer, healthier lives for ourselves, our elder parents, and our children. We want to counter present and future threats to our national security with better technology than that of our adversaries. We want to transform the difficult and complex problems of energy, food, and water supplies, and of protecting the global environment into feasible paths forward."
- **Research Is a National Investment.** "Studies of both the U.S. economy over time and of the economies of our economic competitors consistently show that investment in scientific research pays off. Robert Solow's pioneering study showed that more than half, and perhaps as much as 85 percent, of productivity growth in the U.S. in the first half of the 20th century could be attributed to technical advances. Other studies indicate that 50 percent or more of the nearly sevenfold real growth the country has enjoyed since the end of World War II has been attributable to technological innovation resulting from investments in research and development."
- **A Global Reorganization of Research Is Happening.** "In a globalized economy, international competition in the private sector drives structural changes in national economies. . . . When international competition is fierce, private firms will be more interested in R&D investments that give them an immediate competitive advantage and therefore will choose to invest preferentially in low-risk endeavors—those closer to the development and implementation end of the spectrum. This aspect of globalization has hit basic research done by industry particularly hard. Beginning with the rapid expansion of global competition in the 1990s and the new focus on shareholder value, support by U.S. industry for basic and early applied research has stagnated relative to investments in short-term development."
- **Universities Are Becoming Central Hubs of the Innovation Ecosystem.** "With the decline of investment in research by industry and specialized research laboratories, U.S. research universities are today performing not only the basic research for which they have been best known during the last 50 years but, to an increasing extent, applied and translational research with the potential to deliver innovations, new industries, and market efficiencies over the next 50 years. Today, American research

universities are closer to the marketplace than they have ever been, with a focus on translating and transferring research discoveries to industry."

The document states that "times of transformation are also times of opportunity." These include:

1. Maintain the nation's world-leading position in R&D investment, but better structured as a partnership among industry, government, academia, and others.
2. Adopt policies that enhance the federal government's role as the enduring foundational investor in basic and early-stage applied research.
3. Encourage research portfolios at the agency level that "more strategically support a mix of evolutionary vs. revolutionary research; disciplinary vs. interdisciplinary work; and project-based vs. people-based awards."
4. Adopt policies that better encourage and incentivize industry investment in research.
5. Encourage universities to better prepare their graduates for work in today's world.

An Innovation Strategy for the "45" Administration

Given the importance of innovation to the nation's future and the role of the federal government within the innovation ecosystem, the next presidential administration will need its own innovation strategy. The strategy should strive to successfully balance multiple aspects, for example:

- Encourage current innovation, while also strengthening the foundation for future innovation.
- Address big-picture issues, while also focusing on specific opportunities that are strategically important.
- Accelerate innovation as much as possible, while also enacting policies that protect and encourage implementation of concepts that haven't yet been imagined.

Presidential administrations have a variety of levers at their disposal to support innovation: allocation of federal funds, developing policies that vector private sector activities in a strategic direction, representing U.S. interests on the world stage, and serving as a champion for a number of critically important functional areas and S&T topics.

The rest of this document provides an overview of the global and national innovation ecosystem and looks at the individual landscapes of seven specific areas that will require attention by the next administration. This information can serve as a starting point for deliberations on federal innovation priorities and policies for the nation's future.

The Innovation Landscape

Innovation rarely occurs in a vacuum but rather builds on the successes and failures of prior work by a variety of researchers. The purpose of this section is to provide an overview of the innovation ecosystem at various levels, which is an important step toward understanding future opportunities and challenges for the federal government.

The overall landscape discussed in this chapter and the focused landscapes that appear later in this report indicate sources of innovation that the federal government can leverage to carry out its public mission in novel ways. These chapters also highlight areas in which the federal government can exert influence to drive innovation. It can do so through direct or indirect funding (i.e., funding research or acting as the "leading edge" acquirer of capability) and through policy, regulation, or standardization.

The Global Innovation Landscape

> Globalization of R&D has accelerated in the past decade through a combination of R&D funding growth in emerging economies, off-shoring and outsourcing of a portion of western R&D, improved communications and the need for larger-scale, interdisciplinary, collaboration on major scientific challenges.
>
> —Battelle and R&D Magazine, 2014 Global R&D Funding Forecast (2013)

In 2013, Battelle and *R&D Magazine* projected [20] that the 2014 global innovation investment would reach $1.6 trillion (T). The largest investor was the United States at 31 percent, a drop from 34 percent in 2009. China was the second largest investor at 17.5 percent, a rise from 10 percent in 2009. The next largest investors were Japan (10.2 percent) and Germany (5.7 percent). These top four national investors represent nearly 65 percent of the total worldwide innovation investment. The top 10 countries represent 80 percent. Countries in Africa, the Middle East, South America, and Russia collectively account for approximately 5 percent of global innovation.

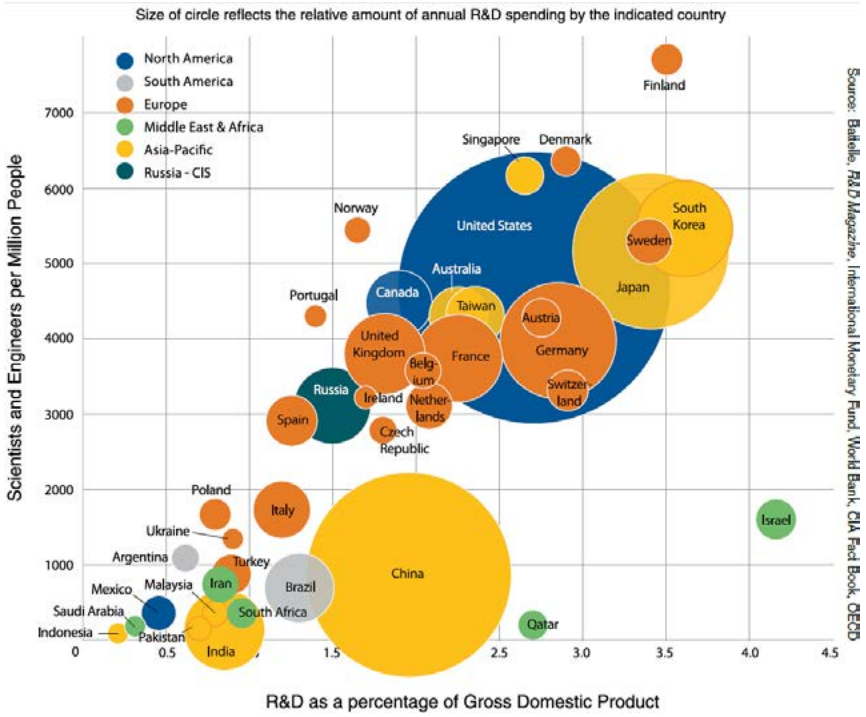

Figure 2. Global R&D Talent and Treasure [20]

China intends to increase its R&D investment (as a percentage of GDP) from the current 1.95 percent to 2.2 percent, while simultaneously transitioning from a predominantly manufacturing-based economy to an innovation driven one by 2020. Meeting this target suggests an ascendancy to the top national innovation position by 2022.

Individual countries have different priorities for research [21] and technology areas. The United States and Europe invest proportionally about three times as much in basic research as China, which places its emphasis on development. India, South Korea, Russia, and Australia are also making notable investments in basic R&D. Researcher-ranked global innovation leaders by individual technology area are shown in Figure 3.

Figure 3. Country Leadership by Technology [20]

The National Innovation Landscape

> Scientific discovery, technological breakthroughs, and innovation are the primary engines for expanding the frontiers of human knowledge and are vital for responding to the challenges and opportunities of the 21st century. The Nation depends on science, technology, and innovation to promote economic growth and job creation, maintain a safe and sufficient food supply, improve the health of Americans, move toward a clean energy future, address global climate change, manage competing demands on environmental resources, and ensure the Nation's security.
>
> —Executive Office of the President, *Multi-Agency S&T Priorities for the FY2017 Budget* (2015)

Battelle and *R&D Magazine* projected the 2014 U.S. innovation investment to reach $465 billion (B), which represents 2.8 percent of GDP. Figure 4 first shows a breakdown of the estimated sources of this investment, followed by estimates of entities that actually performed the research. Industry remains the predominant source (66 percent) and performer (71 percent) of U.S. R&D, with the federal government a distant second at 26 percent and 12 percent (when including Federally Funded Research and Development Centers [FFRDCs]), respectively.

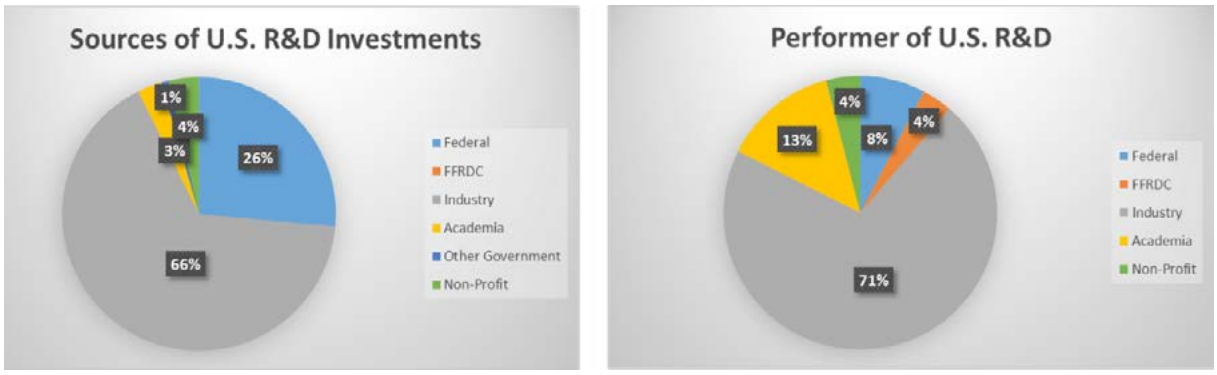

Figure 4. Source and Performer of U.S. R&D [20]

Federal Innovation Landscape

Figure 5 provides a snapshot of the federal government's defense and non-defense R&D budgets since 1977 (in constant 2014 dollars). The American Association for the Advancement of Science (AAAS) groups the trend over the past 15 years into three distinct phases:

1. Fiscal Year (FY) 00 – FY04: Rapid increase (38.5 percent) in federal R&D, primarily driven by an increase in the Department of Defense (DoD) budget following 9/11 and the bipartisan budget doubling at the National Institutes of Health (NIH).
2. FY04 – FY10: Overall steady-state (ignoring one-time American Recovery & Reinvestment Act [ARRA] boost). The DoD budget remained high, while most other budgets began to erode.
3. FY10 – FY15: Steady decline (15.4 percent) in federal R&D. The DoD was hit particularly hard with a decline of 24.1 percent, while non-defense R&D has only declined 4.9 percent.

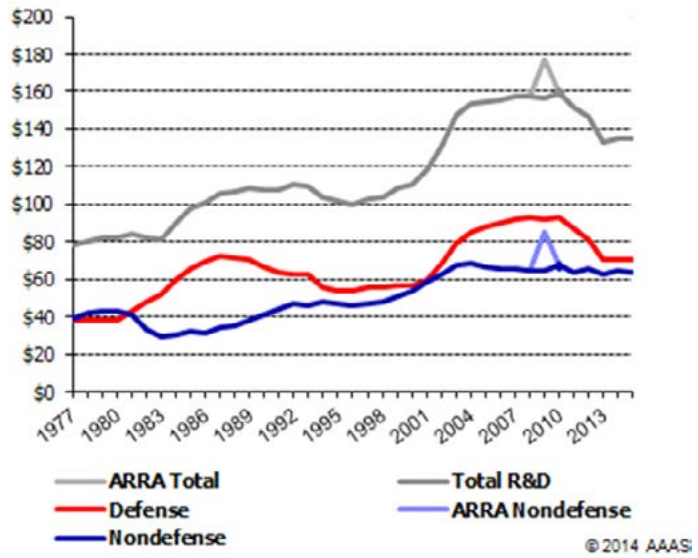

Figure 5. Federal R&D Budgets (Billions in Constant 2014 Dollars)

The National Science Foundation's annual analysis of federal budgets provides a further breakdown by typical R&D Budget Functions, in millions of dollars, as shown in Table 1.

The FY15 R&D budget, as allocated to major agencies, is shown in Figure 6.

Table 1. Federal Budget in $ Millions (M)

R&D Budget Functions	2010	2012	2014
National Defense	86789	79875	70724
Health	31693	31411	31196
Space	8232	10801	11015
General Science & Basic	10509	10536	10207
Energy	2570	2231	2399
Natural Resources & Environment	2430	2300	2378
Agriculture	2206	2005	2088
Transportation	1517	1511	1367
Veterans benefits/services	1034	1160	1173
Commerce & Housing Credits	668	698	1006
Administration of Justice	318	143	1067
Education/training	581	640	570
International Affairs	194	269	280
Medicare	36	80	71
Community/Regional Development	109	58	66
Income Security	77	18	58

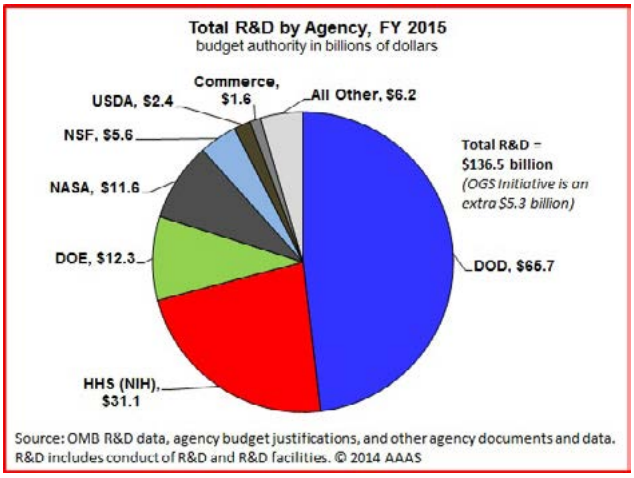

Figure 6. Total R&D by Agency, FY15

Industry Innovation Landscape

The National Science Foundation's *Business Research and Development and Innovation Survey* [22] is the "primary source of information on research and development performed

or funded by businesses within the U.S." Its most recent report found that U.S. companies spent $302B on R&D in 2012, an increase of 2.8 percent over 2011 levels. Manufacturing companies performed $208B of domestic R&D, while non-manufacturing companies performed $94B. For both, 82 percent of their R&D funding came from internal sources (see Figure 7).

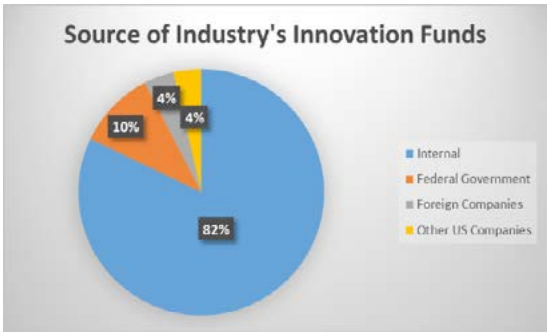

Figure 7. Source of Industry's Innovation Funds (2012)

The U.S. government was the private sector's primary source for external funding ($31B or 56 percent of all external funding), with $25B coming from the DoD. Aerospace, professional/scientific/technical services, and computer/electronics represented 89 percent of the federal government's investment in private-sector innovation.

Innovation-focused companies employed 18.3 million individuals during 2012, with 8 percent dedicated to an R&D job function. Table 2 provides a breakdown of the percentage of total U.S. commercial expenditures and S&T employees by company size in 2012. Numbers from 2009 are roughly similar, with each measure being within a percentage point (plus or minus) of those presented in 2012

Table 2. Percentage of U.S Commercial Expenditures and S&T Employees by Size of Company

Number of Employees	R&D Expenditures	R&D-Focused Employees
5-24	3%	8%
25-49	2%	5%
50-99	3%	5%
100-249	4%	7%
250-499	4%	5%
500-999	4%	5%
1000-4999	17%	15%
5000-9999	10%	9%
10000-24999	16%	13%
25000 or more	36%	27%

> "Entrepreneurs embody the promise of America: the idea that if you have a good idea and are willing to work hard and see it through, you can succeed in this country. And in fulfilling this promise, entrepreneurs also play a critical role in expanding our economy and creating jobs."
>
> —President Barack Obama, January 31, 2011

Business R&D is predominantly concentrated in a handful of states, dominated by California, which accounted for 27 percent of the nation's commercial R&D. Only three other states contributed 5 percent or more: Massachusetts (5.8 percent), New Jersey (5.2 percent), and Texas (5.0 percent). The top 10 states collectively contributed 66.6 percent of the entire nation's commercial innovation investment.

The key areas for commercial R&D within the United States are shown in Table 3.

Table 3. Percentage of Total U.S. Commercial R&D

R&D Focus Areas	2009	2012
Pharmaceuticals and Medicine	15.9%	15.9%
Machinery	3.2%	4.7%
Computer and Electronics Manufacturing	21.4%	21.5%
Transportation Equipment	17.1%	14.0%
Information Technology	12.0%	15.5%
Finance and Insurance	0.7%	1.2%
Computer Systems Design	4.4%	3.7%
Basic and Early Applied	6.1%	5.5%

The venture capital community also plays an important role in the innovation ecosystem. "Investment levels in 2014 were remarkable in that they were the highest amount since 2000, and the third-highest ever at $49.3B. This compares with $30.1B in 2013, which was in line with the prior several years" [23]. A further historical perspective from the National Capital Venture Association is shown in Figure 8, while Figure 9 provides a breakdown of investments by technology area in 2014.

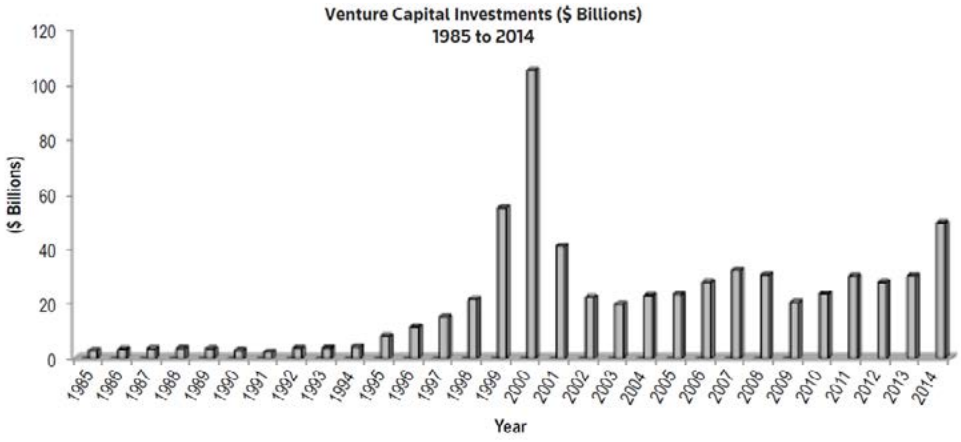

Figure 8. Historical Venture Capital Investments [23]

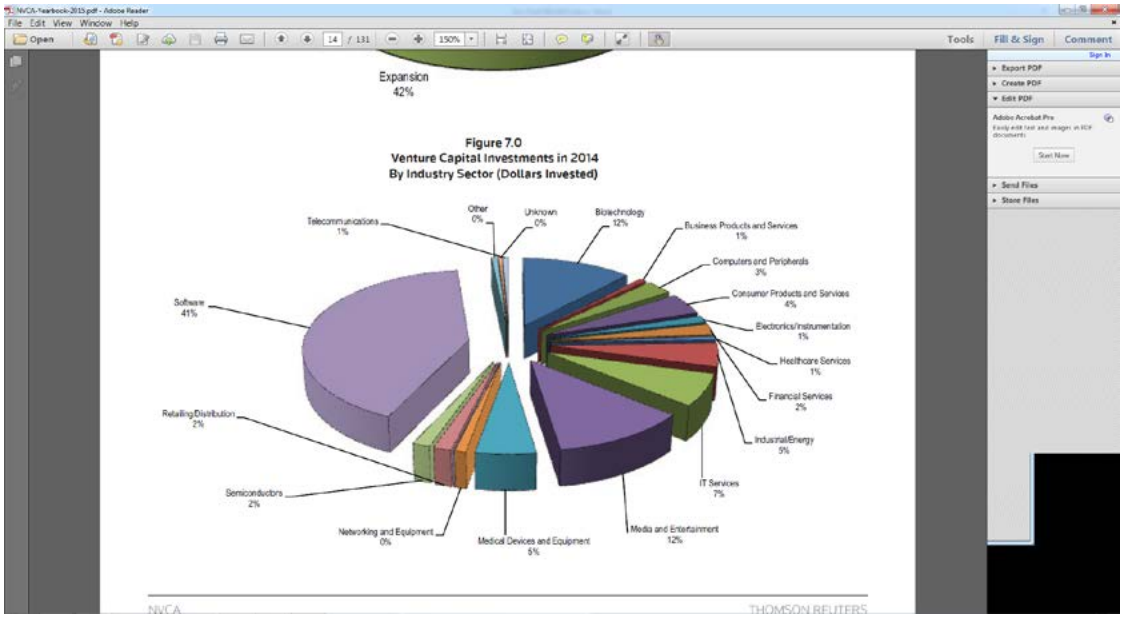

Figure 9. Venture Capital Investments in 2014 [23]

Academic Innovation Landscape

America's research universities serve a dual role in the national innovation ecosystem as they perform 60 percent of the nation's basic research and also train the nation's future innovators. This current reliance on universities came about by design. Prior to World War II, most basic and early-stage applied research was performed by industry. The shift toward universities began during World War II when they began playing critical roles in the war effort by developing new technologies, such as radar, penicillin, and the atomic bomb. Vannevar Bush's 1945 report, *Science: The Endless Frontier*, called for a new partnership in which basic research would increasingly be funded by the federal government and performed in universities. This partnership has continued to grow; today, approximately 200 universities award innovation-based doctorates and/or manage more than $35M in R&D [24].

From a global perspective, American universities continue to be at the forefront of academically performed innovation. The Academic Ranking of World Universities [25] develops an annual ranking of the world's research universities based on a set of six criteria, such as the number of Nobel Prizes awarded, number of articles published in top journals, and the number of research citations. According to its 2014 rankings, the United States housed eight of the top 10 and 18 of the top 25 research universities worldwide.

These rankings are not assured in the future, however. The National Academies of Science (NAS) determined in 2012 that "research universities confront critical pressures, including unstable revenue streams, demographic shifts in the U.S. population, changes in the organization and scale of research, and shifting relationships between research universities, government, and industry. Research universities also face growing competition from their

counterparts abroad . . . . (as) other countries are rapidly strengthening their institutions to compete for the best international students, and for faculty, resources, and reputation" [24].

> It is essential that we as a nation reaffirm, revitalize, and strengthen substantially the unique partnership that has long existed among the nation's research universities, the federal government, the states, and philanthropy… In doing so, we will encourage the ideas and innovations that will lead to more high-end jobs, increased incomes, and the national security, health, and prosperity we expect.
>
> —National Academies of Science, *Research Universities and the Future of America* (2012)

The NAS provided 10 recommendations to accomplish three broad goals, as follows:

- Revitalizing partnerships among universities and other members of the innovation ecosystem:
  - The federal government should adopt stable and effective policies, practices, and funding for university–performed R&D and graduate education.
  - States should provide greater autonomy for public research universities so that they can leverage local and regional strengths to compete strategically and be agile enough to quickly act on new opportunities.
  - The partnership between universities and industry should be strengthened so that new discoveries are transferred to achieve national goals.
  - Universities should increase their cost–effectiveness and productivity so their partners receive a higher return on investment.
- Streamline and improve the productivity of research within universities:
  - The federal government should create a "Strategic Investment Program" that funds initiatives critical to advancing education and research in areas of national priority.
  - Academic research sponsors should strive to cover the full costs of research projects at universities, so that they don't have to subsidize research from other sources.
  - Federal and state governments should review the costs and benefits of regulations and remove those that are redundant, ineffective, inappropriately applied to higher education, or that impose costs that outweigh benefits.
- Ensure that America's pipeline of researchers remains flowing:
  - Research universities should improve the capacity of graduate programs to attract students by addressing issues such as attrition rates, time to degree, funding, and alignment with career opportunities and national interests.
  - The nation needs to enhance STEM pathways and diversity to attract more students.
  - Government must ensure that universities and the nation benefit from the participation of international students and scholars.

> The United States is losing its competitive edge in math and science while the rest of the world soars ahead. Our knowledge capital, which fuels innovation and economic growth, is at risk.
>
> ——–The National Math + Science Initiative

The Nation's STEM Crisis

The President's Council of Advisors on Science and Technology (PCAST) wrote that "(e) conomic projections point to a need for approximately 1 million more STEM professionals than the U.S. will produce at the current rate over the next decade if the country is to retain its historical preeminence in science and technology. To meet this goal, the United States will need to increase the number of students who receive undergraduate STEM degrees by about 34 percent annually over current rates" [26].

The previous section outlined the extremely high regard that U.S. research universities hold on the world stage, yet those rankings overshadow important gaps in the future U.S. innovation workforce. Foreign students, who earned only 11.6 percent of all U.S. doctorates in the 2012–2013 academic year, earned:

- 57 percent of doctoral degrees conferred in engineering
- 53 percent of doctoral degrees conferred in computer and information sciences
- 50 percent of doctoral degrees conferred in mathematics and statistics [27]

This trend is also seen at the baccalaureate level. Foreign students made up only 3.5 percent of Bachelor of Science (B.S.) degrees earned, but 10 percent of those in mathematics and 8 percent of engineering degrees [27]. During the 2013–2014 academic year, nearly 900,000 students from other countries were enrolled in U.S. colleges or universities. This represents a 72 percent gain from 1999 levels, as shown in Figure 10 [27].

Cybersecurity is one of the STEM fields suffering from a lack of interest among students and millennials. "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million," says Symantec Chief Executive Officer (CEO) Michael Brown. The "Cisco 2014 Annual Security Report" warned that the worldwide shortage of information security professionals is at 1 million openings, even as cyberattacks and data breaches increase each year. Industry experts suggest that we have to engage not only college students in cybersecurity and other STEM topics, but younger students as well, if we are to close the gap between openings and qualified applicants.

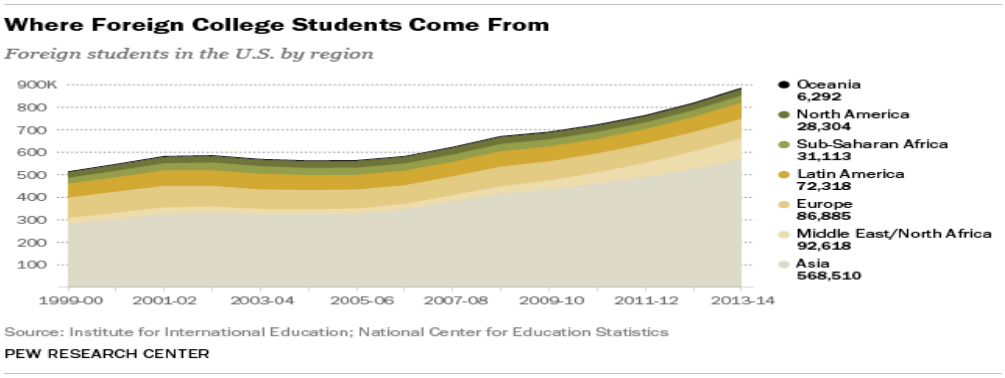

Figure 10. Where Foreign College Students Come from (Institute of International Education)

The United States enrolls more international students in STEM fields than the United Kingdom (U.K.), Australia, and Canada combined, and the percentage of foreign students within overall U.S. academic enrollments is the highest worldwide at 37 percent (26 percent for the U.K., 25 percent for Canada, and 21 percent for Australia) [28]. Policy changes, such as the extension of "Optional Practical Training"[1] [29] for international STEM graduates has fueled foreign interest in studying in the United States over the past 10 years. This program is only a short-term fix, however, which would not be needed if the U.S. talent pipeline were enhanced.

For example, fewer than 40 percent of U.S. students who enter college intending to major in a STEM field actually complete a STEM degree [18]. Simply improving this rate to 50 percent would generate 750,000 new STEM graduates. According to PCAST, "High performing students frequently cite uninspiring introductory courses as a factor in their choice to switch majors. And low-performing students with a high interest and aptitude in STEM careers often have difficulty with the math required in introductory STEM courses, with little help provided by their universities."

A further disheartening aspect of U.S. STEM education is that women and minorities represent 70 percent of all college students but only 45 percent of those graduating with a STEM degree [18]. In the workforce, women represent 48 percent of all workers, but only 23 percent of those within STEM fields [30].

1. This extends the visa timeframe for those earning STEM degrees. See: [29].

Technology Landscapes

The previous section outlines the important role of innovation within the global and national community. This section provides more in-depth analysis on two operating sectors and four technology areas that will be of particular interest to the next presidential administration.

These six analyses do not represent a summation of emerging technologies[2] [31] nor a consensus on the most transformative technologies of the next dozen years. Rather, they represent a collection of sectors and technologies that will require federal leadership in the near-term to preserve the nation's security and prosperity in the future.

Each analysis is provided in its own subsection so that they can be excerpted for further study. Each includes a basic introduction to the issue, a look at global and national environments, and recommended actions and questions that need additional consideration prior to development of the next administration's strategy.

Operating Sectors

Critical Infrastructure Security and Resilience

Introduction

The U.S. Code defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [32].

Definition of "resilience" varies across domains, but it typically includes the concepts of preparing for an adverse event, withstanding an event, and recovering from the event. In the *2010 Quadrennial Homeland Security Report*, [33] the Department of Homeland Security (DHS) distinguishes between:

- Protecting critical infrastructure ("prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions, including linkages through cyberspace, from attacks or disruption") and
- Making critical infrastructure resilient ("enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions").

Similarly, the National Infrastructure Advisory Council (NIAC) defines infrastructure resilience as "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" [34].

2. Gartner's annual "Hype Cycle for Emerging Technologies" is very informative in this regard. See [31].

Presidential Policy Directive 21 (PPD–21), "Critical Infrastructure Security and Resilience," [35] identifies 17 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. Of these, four are designated by DHS as *lifeline sectors:* communications, energy, transportation systems, and water. These four sectors are so important that a loss of any one could result in significant financial loss as well as loss of life.

The number of these systems and assets across the country is very large. To get a sense of how large, the 2003 *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* [36] estimates that the United States has 300,000 oil and natural gas producing sites, 170,000 public water systems, 120,000 miles of major railroads, 5,800 hospitals, and 104 nuclear power plants. Clearly not every asset is as crucial as the other or would have as significant an impact if compromised; however, these numbers do illustrate the scale of the Critical Infrastructure Security and Resilience (CISR) problem space.

According to PPD–21, "Critical infrastructure provides the essential services that underpin American society" and "proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure." The CISR community is focused on enabling the development of evolutionary and transformative approaches to enhancing the security and resilience of Critical Infrastructure (CI) systems, whether these systems face threats that are manmade (such as a physical– or cyber–attack) or natural (such as a hurricane or pandemic).

To emphasize the importance of cybersecurity in CI, Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," [37] states that security and resilience goals can be achieved "through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk–based standards."

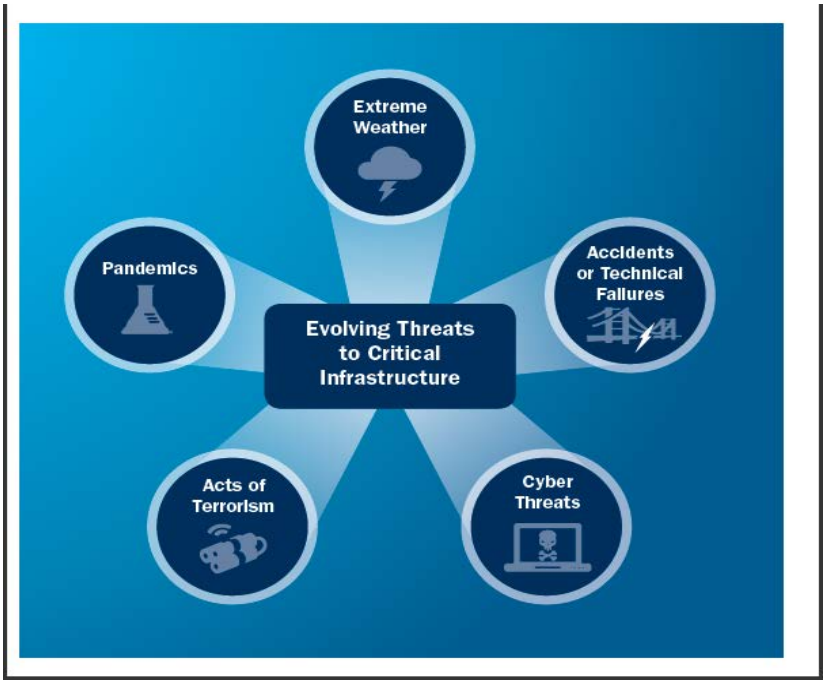

Figure 11. Critical Infrastructure Faces Threats from a Wide and Varied Spectrum

Challenges to CISR

The wide range of possible threats to CI include climate change, aging infrastructure, and acts of terrorism, as well as the increased connectivity and interdependency of our infrastructure (Figure 11). The risk of cyber-attacks continues to grow, due to advanced techniques, multiple potential methods of attack (physical, network, and combined), and the enormous, enduring impacts of a successful system intrusion, which are transforming cyber-physical systems (CPS) attacks into low-risk, low-cost, high-impact endeavors. In addition, business efficiencies and industry consolidation can actually increase the number of single points of failure in CI.

The loss of capability or functionality in a single sector can cascade to impact many individuals and geographic regions, and may cause repercussions in other sectors, leading to higher losses. For example, a large electrical outage could easily cascade across sectors, impacting water service, hospitals, transportation, and the food supply.

More specifically, as a result of the 9/11 attacks in New York City, the fire, structural failure, and subsequent collapse of the World Trade Center (WTC) towers caused the water lines to rupture, causing water to flow out of the broken water mains beneath and around the disaster (Figure 12). This knocked out a very large communications hub (directly impacting the financial services sector), limited water to emergency services trying to fight fires, and flooded subway and commuter lines. The cascading failure blurred the lines between physical and cyber and ultimately led to additional loss of life.

Recently, the University of Cambridge and Lloyd's published the "Business Blackout" report, which depicts hypothetical, yet realistic, scenarios that could affect the U.S. electric grid. These include cyber–attacks on the grid, which could result in cascading effects across the lifeline sectors [38].

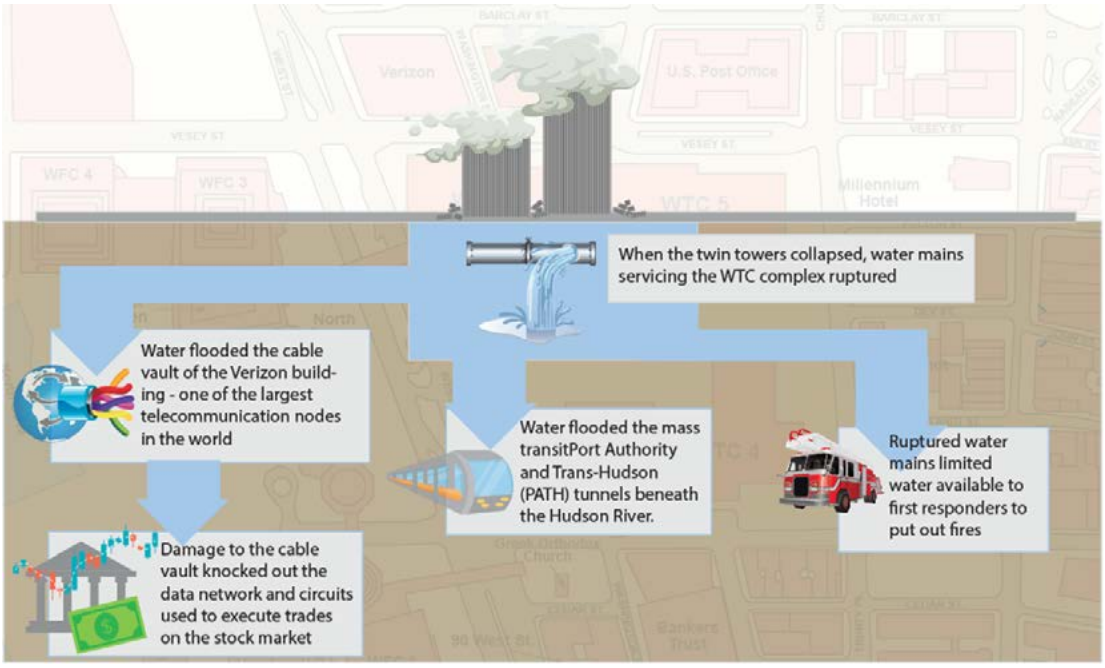

Figure 12. Connectivity and Interdependency of Critical Infrastructure Sectors Can Lead to Cascading Failures

Resilience objectives include securing lifeline functions and making progress against emerging threats and reducing the risk of the largest–scale potential failures. Achieving resilience is more complex than traditional protection efforts as it requires more systemic understanding of acceptable levels of risk against cost and missed opportunities. The United States must weigh the ability of infrastructure to withstand and recover from various events against the willingness and ability of government and operators (in addition to the public) to invest materially in resilience beforehand.

Scope of CISR

The nation's critical infrastructure comprises a complex, highly–interconnected and distributed system–of–systems (SoS). While each individual sector protects its own SoS, vulnerabilities also exist at the interface(s) between sectors. Thus, the outcome of a CISR strategic approach is a more secure SoS that prevents or withstands attacks, thereby reducing the likelihood and impact of a large–scale disruption of critical services to millions of Americans.

Of critical importance to this CISR strategy is the recognition that the government is not in a position, nor does it have the legal authorities, to directly address all potential CISR vulnerabilities and challenges faced by civilian and defense agencies, as 85–90 percent [39] of the CI in the United States is owned by the private sector. The government has the ability to

develop standards, issue regulations, and provide funding to address CISR needs. However, to achieve enduring resilience, the government and the private sector must jointly identify the most significant CISR issues and work together to identify priorities, required resources, strategic partners, and outcomes. Outcomes should include greater cyber–physical security, advanced threat detection and mitigation, and advanced capabilities to withstand, respond to, and recover from CPS attacks.

Military bases are a good example of why public and private entities must work together to ensure national security. Successful base operations and force protection require both the availability and surge capacity of the local, civilian–owned and operated CI that supports the base. While an identified vulnerability in one node of a civilian–owned CI that has limited or no impact on the success of base operations is not a likely target for federal government investment, it may be an appropriate area for industry investment. A potentially critical vulnerability that could impact multiple facets of base operations, however, may be an area in which the federal government should invest; a regional attack on a lifeline sector across a militarily significant region containing many bases or defense industrial base companies could have national security implications.

A resilience strategy spans the time around a potential event, as there are components of resilience that occur before, during, and following the event: resistance (preventing loss), absorption (minimizing loss), and recovery (regaining from loss). Being able to predict a threat or crisis before it occurs can sometimes trigger preventative measures that mitigate the impact or possibly forestall the event. The ability of CI to withstand an actual event depends on advanced planning. What happens after an event is also critical as recovery may be dictated by public–private policies, plans, and practices. Finally, a resilient CI must adapt and evolve to keep pace with the changing threat landscape.

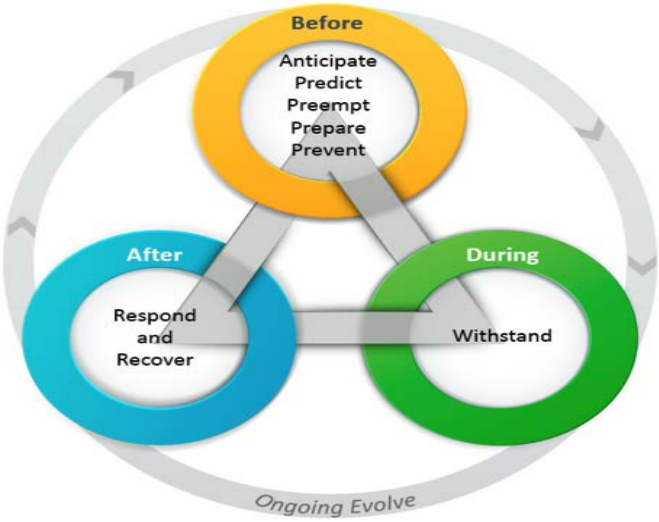

Figure 13. Resiliency Practices Address Four Elements: Anticipate, Withstand, Recover, and Evolve

A wide range of technologies contribute significantly to CISR, covering cyber and physical systems, as well as interdependencies. Building a strategy, therefore, requires the identification of enhanced key capabilities to be addressed, including technical means (e.g., advanced surveillance systems for CI facilities and emerging cyber resilience techniques), tools (e.g., those that support situational awareness, collaboration, and rapid, adaptive deployment of crews and materiel), and modeling and analysis techniques to support scenario assessment and planning.

Goals of a CISR Strategy

The top-level goals of a robust CISR strategy include:

1. Develop a foundational understanding of CI systems and systems dynamics that takes into account both intra-sector and cross-sector dependencies and focuses on critical gaps and challenges across lifeline and critical functions. Of particular interest is an understanding of cascading disruptions across multiple CI systems within a region, as well as factors that contribute to, prevent, or mitigate these disruptions.
2. Develop a comprehensive understanding of interdependencies, as well as scalable and integrated risk assessment, resilience, and management tools, to support decisions involving CI resilience in critical areas. This includes the development of metrics for infrastructure resilience and the application of them to measure national and regional resilience.
3. Develop capabilities, technologies, and methods to enable more secure and resilient infrastructures that are able to withstand and recover more effectively from large-scale failures.
4. Develop early adoption and acceptance of technology advancements, including integrated situational awareness across sectors, via techniques such as leveraging advancements in big data analytics, sensors, and signal processing technologies.

While other areas of investigation are also important, e.g., assessing the impact of policies, budgets, and regulations on resilience and innovation, there is general agreement that the preceding topics are key to improving CISR.

Landscapes

Quantifying the R&D investment in CISR is difficult because such funding is not always easily distinguished from other R&D research performed by various industries or government agencies. The research literature, however, can be used to estimate activity and engagement, examining and identifying the various organizations (both domestically and abroad) that are publishing in this field, as well as the topic areas of interest. Of course there are entities performing CISR research that are not concerned with publishing in the open literature and, as such, findings based on any literature search may not paint a complete and accurate picture of the CISR landscape.

Global Landscape

The security and resilience of CI is a concern for all nations, albeit to varying degrees for some sectors. For example, while energy is a common CI for all nations, the dominant source of energy may vary. Norway almost exclusively uses hydroelectric sources for its electricity, while the bulk of China's electricity is generated by burning coal.

CISR considerations also depend on whether or not the energy commodity under consideration is consumed domestically or is exported. Recently, Russia, has seen a drop in the domestic consumption of natural gas to generate electricity since the industry can increase its profits significantly by exporting the gas. As a result, Russia has increased its use of other technologies, including nuclear power, resulting in new CISR challenges.

Other considerations include the domestic availability of energy sources and the number of generation stations in use (along with the respective size of any dominant sources). For example, the Temelín Nuclear Power Station in the Czech Republic produces 15 to 20 percent of the total electricity generated in the country, which has fewer than 35 stations with capacity greater than 100 megawatts (MW). The loss of that single facility would have a dramatic impact across all facets of life in the region.

We conducted a literature search to identify research efforts germane to infrastructure resilience, particularly for multiple infrastructures, cascading disruptions, and supervisory control and data acquisition (SCADA) systems. As expected, a wide range of countries were conducting research, in addition to the United States: Italy, Australia, France, the U.K., Canada, Germany, China, India, the Netherlands, and Sweden, among many others. While this isn't a complete picture of the work transpiring in CISR, it does indicate how widely recognized CISR is as an area of concern.

Of all the infrastructures considered, the power grid seems to command the most interest. As an example, there is work from India, South Africa, and the Czech Republic focused on "system protection schemes" and vulnerabilities of national grids. In addition to the energy and Information Technology (IT)/communication sectors, other infrastructures of concern include water and transportation (i.e., the lifeline sectors).

National Landscape

A large number of players within the United States are working on various CISR-related topics, including universities, national laboratories, government organizations, FFRDCs, and commercial entities.

Reflecting the fact that there are CI dependencies at the system, local, regional, and national levels, Sector-Specific Agencies (SSA) and sector stakeholders undertake R&D activities in CPS security, as appropriate to their unique risk and operating environments. Many CI systems involve CPS and thus offer opportunities to address the increasing autonomy and cooperation possible while providing greater assurances of safety, security, scalability, and reliability.

PPD–21 notes, "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient." Further, the 2013 National Infrastructure Protection Plan (NIPP) [40] states that "given the diverse authorities, roles, and responsibilities of critical infrastructure partners, flexible, proactive, and inclusive partnerships are required to advance critical infrastructure security and resilience."

The NIPP then states that "Individual efforts to manage risk are enhanced by a collaborative public–private partnership that operates as a unified national effort, as opposed to a hierarchical, command–and–control structure." Further, the NIPP details sector and cross–sector partnership council structures as shown in Table 4.

Table 4. Sector and Cross–sector Coordinating Structure (NIPP)

		Critical Infrastructure Partnership Advisory Council		
Critical Infrastructure Sector	**Sector-Specific Agency**	**Sector Coordinating Councils (SCCs)**	**Government Coordinating Councils (GCCs)**	**Regional Consortia**
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ		✓	✓	
Communications ⓘ		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services ⓘ		✓	✓	
Information Technology ⓘ		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Academic Landscape

Our literature scan revealed a number of universities that appear more than once in the CISR papers that were reviewed, including Carnegie Mellon, which has a new CERT Cyber Resilience Center and a Resilience Management Model (RMM) within its Software Engineering Institute (SEI). Arizona State University's (ASU's) new ASU Decision Theater Network was built to address cross-disciplinary local, national, and international issues, applying expertise in collaborative computing and display technologies for data visualization and modeling and simulation. Its research has included work on secure and resilient societies, as well as on complex systems. Virginia Tech's Advanced Research Institute is engaged in research on the Smart Grid, alternative energies, and disaster risk reduction.

The University of Virginia Center for Risk Management of Engineering Systems develops theory, methodology, and technology to assist in the risk management in a variety of engineering systems, including our nation's critical infrastructures. Other universities, including the Florida Institute of Technology, George Mason University (through its Center for Infrastructure Protection and Homeland Security), Northeastern University (through the Kostas Research Institute for Homeland Security), and Ohio State University, are also active in aspects of CISR. Other highly published (and cited) papers came from authors at the University of Tulsa, the Naval Postgraduate School, and Yale University.

Government Landscape

As shown in Table 4, each of the nation's 16 CI sectors has a Sector-Specific Agency that is charged with carrying out roles and responsibilities for their sector(s). As a result, multiple federal departments and agencies sponsor research on CISR, most prominently the Department of Energy (DOE) and DHS. As mentioned previously, the DoD is also concerned with various aspects of infrastructure, particularly electricity, security, and resilience at its many bases, as well as supporting the defense industrial base. Similarly, NIST and the National Science Foundation (NSF) are also interested in various aspects of resilience.

DOE established the National SCADA Test Bed (NSTB) at Idaho National Lab (INL) and Sandia National Lab (SNL). The NSTB includes an 890-square mile CI Test Range, complete with industrial scale infrastructure components that can be used for conducting comprehensive interoperability, vulnerability, and risk assessments. While some research on developing security for SCADA systems was identified at INL, the main purpose of the NSTB is to provide a test bed environment for evaluating commercial off-the-shelf (COTS) SCADA systems.

The Air Force Institute of Technology (AFIT) at Wright-Patterson Air Force Base is also looking into the security of SCADA systems. Although there is a body of research focused on the security of SCADA systems, at this time no one can claim to have solved the problem. Part of the problem is that there are countless varieties of SCADA systems, very few of which are presumed to be secure.

DHS recognizes that "the security of the nation's critical infrastructure requires an effective partnership framework that fosters integrated, collaborative engagement and interaction among public- and private-sector partners." To this end, the government has established several public-private partnerships in addition to NIAC, including: the Critical Infrastructure Partnership Advisory Council, Sector Coordinating Councils, Government Coordinating Councils, the Critical Infrastructure Cross-Sector Council, the Federal Senior Leadership Council, the State, Local, Tribal, and Territorial Government Coordinating Council, and the Regional Consortium Coordinating Council. The 2013 NIPP has greater detail on the sector and cross-sector council structures; see [40] "Appendix A. The National Partnership Structure".

Industry Landscape

The government owns and controls very few CI assets in the United States. The vast majority is owned and/or operated by the private and non-profit sectors. The energy/electric power subsector supports a not-for-profit research institute, the Electric Power Research Institute (EPRI), which is funded by electric power company members. EPRI seeks to develop "innovative solutions that enable the transformation of power systems to be more flexible, resilient and connected, to provide society with safe, reliable, affordable and environmentally responsible electricity" [41]. EPRI's results are used in commercial products, where possible, or otherwise made available for members' use.

Among the projects in EPRI's 2015 research portfolio are some for Grid Operations and Planning. This includes Transmission Contingency and Reliability Evaluation (TransCARE), "software that provides a comprehensive framework for computing reliability indices for transmission networks, identifying worst-case contingencies and impacts of remedial action schemes, analyzing costs and benefits for various transmission upgrade options, studying the impacts of variable generation on system reliability, and analyzing extreme events, as well as performing NERC [North American Electric Reliability Corporation] compliance studies." The estimated 2015 funding for the program is $2.5M [41].[3] Among many other projects, EPRI is conducting studies on more efficient water use in power plants since both conventional and nuclear plants are major users of water.

Fourteen of the CI sectors are served by Information Sharing and Analysis Centers (ISACs), trusted entities that have been established and are operated by CI owners and operators. The mission of the various ISACs is to further the cyber- and physical security of the CI sectors and provide a mechanism for data sharing among members as well as with the government.

Research Landscape

As discussed, there are hundreds of institutions participating in advancing CISR. This includes a large number of universities, the national laboratories, as well as various government organizations and commercial entities within the United States. There are emerging

3. The TransCARE Program Manager is D. Brooks, 865-218-8040, dbrooks@epri.com.

centers of expertise in simulation and industrial controls; and there are emerging areas of research in the security of intelligent transportation infrastructure, data driven infrastructure provisioning, and dynamic cloud communications infrastructure.

To better understand the relevancy of these efforts to CISR, it is useful to distinguish between four types of research efforts:

- **Novel:** Cutting-edge work that is both transformational and generation-skipping, leading to potential transformational capabilities.
- **Technology harvesting:** Research that uses existing technologies in novel ways to address both short-term and mid-term program needs.
- **Strategic gap-filling:** Research that uncovers innovation gaps in existing programs and develops and/or co-opts technologies to overcome those gaps.
- **Informational:** Work that is performed to gain first-hand experience but does not lead to new ideas or concepts; its value is to educate and inform.

Table 5 summarizes the major players involved in CI resilience research at the national level along with their respective areas of expertise and types of research performed. The impact of these efforts on the CISR strategy top-level goals is also noted.

Table 5. CI Resilience Research (NIPP)

Entity	Area	Research Type	CISR Strategy Goal
AFIT	Industrial Control Systems (ICS)/ Cyber Resilience	Harvesting/Gap-Filling	3,4
ASU	Decision Support	Harvesting	1,2,4
Carnegie Mellon	Cyber Resilience	Novel	3
EPRI	Risk/Reliability Assessment	Harvesting/Gap-Filling	3,4
INL	ICS/Cross-sector M&S	Novel/Harvesting	1,3
Los Alamos National Lab (LANL)	Cross-sector M&S	Novel/Harvesting	1,3
MITRE	Cyber Resilience/GPS	Novel/Harvesting/Gap-Filling	3
NERC	Power Grid/Cyber Resilience	Harvesting/Gap-Filling	1,3,4
Oak Ridge National Laboratory (ORNL)	Cross-sector M&S	Novel/Harvesting	1,3
Pacific Northwest National Laboratory (PNNL)	Cross-sector M&S	Harvesting/Gap-Filling	1,3,4
Santa Fe Institute (SFI)	Complex Networks	Novel	1
SNL	ICS/Cross-sector M&S	Novel/Harvesting	1,3
University of Virginia (UVA)	Risk/Reliability Assessment	Novel/Harvesting	2
VA Tech	Smart Grid/Alt. Energy	Novel	1,2,3,4

In June 2015, DHS announced that it had selected the University of Illinois at Urbana-Champaign as the lead institution to establish a new Critical Infrastructure Resilience Center of Excellence (COE). The Critical Infrastructure Resilience Institute (CIRI) "will conduct research and education to enhance the resiliency of the Nation's critical infrastructures and the businesses and public entities that own and operate those assets and systems. A significant focus of the CIRI will be on transitioning research outputs for use by DHS operational

components, other homeland security end users, policy makers, decision makers across all levels of industry and government, and community leaders" [42].

The formation of CIRI followed the establishment of a Coastal Resilience COE led by the University of North Carolina at Chapel Hill. Some CISR-related research may also be conducted in some of the other nine COEs that DHS sponsors.

In general, the government organizations concerned with CISR do not conduct research in-house but rather fund national laboratories and/or universities for that purpose (thus explaining the absence of these entities in the Table 5).

INL and SNL, along with Argonne National Laboratory (ANL), Brookhaven National Laboratory (BNL), Pacific Northwest National Laboratory (PNNL), Los Alamos National Lab (LANL), and Oak Ridge National Laboratory (ORNL), all conduct CI resilience research. Some have developed models to address infrastructure interdependencies, including those at the National Infrastructure Simulation and Analysis Center at LANL. It should be noted that these models are very detailed and computationally complex, taking long periods of time (days to weeks) to run. Near-term solutions would be based on more coarsely grained models.

The Santa Fe Institute (SFI) conducts research on complex systems, including interdependent infrastructures. Several SFI associates were members of the Institute of Electrical and Electronics Engineers (IEEE) Computing and Analytical Methods Subcommittee (CAMS) Task Force on Understanding, Prediction, Mitigation, and Restoration of Cascading Failures. The CAMS Task Force produced some comprehensive IEEE reviews on the subject, including "Risk Assessment of Cascading Outages: Part I – Overview of Methodologies," and "Part II, Survey of Tools for Risk Assessment of Cascading Outages."

While industry conducts some level of R&D into CISR, it is difficult to ascertain specific levels of effort. Clearly the specific regulatory environment in which a CI operator exists will determine the ability to innovate and adopt specific CISR technologies (or not). In the cyber area, however, some CI operators are beginning to employ firms that have strong and historical ties to working with the DoD. The hope is that by leveraging some of the tactics, techniques, and procedures (TTPs) developed in that environment, strides can be made to quickly improve cyber resiliency in critical infrastructure.

European countries are generally well represented in power research, but much of their research focuses on developing renewable energies and green energy, rather than on the resilience of present systems. The motto of the European Energy Research Alliance (EERA) is "Coordinating energy research for a low carbon Europe." The European Institute for Energy Research (EIFER) is a joint program of the EDF Group, a major European power company, and the Karlsruhe Institute of Technology. EIFER states that its primary focus is on ". . . delivering research-based innovative energy solutions for the sustainable growth of cities, local communities and industries."

After those in the United States, Italian universities and research centers were most active in published CI resilience research. For example, the Critical Utility Infrastructural Resilience (CRUTIAL) project, formed in 2006, was a partnership led by Italian universities with participation from universities in Portugal, France, and Belgium. The three-year project conducted analyses of critical scenarios, in which faults in the IT infrastructure result in serious damage to the electric power infrastructure. CRUTIAL completed the project by developing new network architectures, resilient to both accidental failures and malicious attacks. CRUTIAL results are the subject of at least 25 journal articles [43].

Looking Forward

A number of CISR areas that be addressed to ensure that continual improvements are made across the various sectors. Some of the biggest challenges to achieving CISR, however, are not technological but rather political and economic. This is seen in the three strategic imperatives set forth in PPD–21, which focus on developing and enhancing capabilities across the federal government:

1. Refine and clarify functional relationships across the federal government to advance the national unity of effort to strengthen critical infrastructure security and resilience.
2. Enable effective information exchange by identifying baseline data and systems requirements for the federal government.
3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

It should be noted that PPD–21 and EO–13636 mandate actions of federal executive branch agencies; they cannot direct action by the private sector. Rather, the EO and PPD encourage industry to adopt cybersecurity measures, including the Cybersecurity Framework, best practices, and security controls that are developed under the direction of both presidential directives.

As was noted in a November 2014 National R&D Plan from the National Infrastructure Advisory Council (NIAC) [44], "Current regulatory frameworks and national policy have not kept pace with the changing landscape of critical infrastructure security and resilience. They are often not harmonized, and do not encourage resilience against the broader geographic impact of catastrophes, nor the growing operational complexity and dependencies of the critical infrastructures." Similarly, it may be difficult and/or time-consuming for funding sources from various aspects and levels of government to be combined.

The EO recognizes that CI owners and operators have to take the primary responsibility for protecting themselves. The EO does not mandate a single CISR standard, nor does it require the use of specific products or services. Rather, the EO seeks to leverage market forces, innovation, and creativity as the desired approach, not one in which the government mandates solutions.

Thus, since the majority of CI assets are owned and operated by the private sector, there is a strong need for incentives (as recognized in EO–13636) that support the adoption of

a variety of CISR technologies and practices. The sheer size of the nation's infrastructure (compounded by its age, in many cases), serves to make CISR improvements an expensive proposition.

The regions and private sector companies that own and operate the bulk of our nation's critical infrastructure have business models in place and are continually seeking ways to improve business operations and improve their economic stability. This set of diverse stakeholders, in general, worries about the functionality of the assets, the ability of their companies to operate day-in and day-out and to provide services and jobs. Concepts such as "up time," return on investment (ROI), and risk are a fundamental part of their deoxyribonucleic acid (DNA). On the other hand, the federal government places a significant focus on protecting assets during high-impact, low-frequency (HILF) events. The two sides need to find common ground—the sweet spot is economically sound and resiliently designed infrastructure – or ways to complement each other without leaving gaps.

One area to address is highlighted in the NIAC: "Policies and regulations can act as disincentives to investments and collaboration across sectors and between public and private sectors. There is often little to no value proposition for investment, either from a political or a commercial perspective. Consequently, appropriate regulations and policies could also act as an enabler."

From a technological perspective, there is demand to develop a common operating picture in the event of a major CI-impacted event. To achieve this, local, state, and federal government entities need to develop effective and efficient methods of sharing information. The concept of increasing and improving information sharing is consistently recognized as a primary component of robust CISR and is thus a key goal of both EO-13636 and PPD-21.

The PPD and EO can only direct the federal government to share information, not the private sector, so the majority of the flow of information is expected to be from government to industry. However, there is nothing in either presidential directive that prohibits the owners and operators of critical infrastructures, specifically within a given sector, from sharing information with each other (as is currently occurring through the various ISACs) and also with the appropriate entities in the various federal, state, and local governments.

Even though there is widespread acknowledgement of and support for this view, it nonetheless, remains an elusive goal. To establish the trusted relationships needed to produce effective sharing mechanisms, various concerns must first be met. Foremost is the question of data access and, specifically, protection of shared proprietary information. Various attempts have been made to address this, including the Protected Critical Infrastructure Information program.

Regional CI Resilience

Because people live and make decisions in the context of their geographic communities, and not in terms of various infrastructure sectors, it makes sense to address CI from a regional perspective.

For example, in the electricity sector there are several large grid operators that help balance transmission, but restoration priorities are typically a negotiation among local distribution companies and the state and local leaders—which also have control over rates. The communications sector is regulated under a combination of federal and (diverse) state rules. Today, the various stakeholders do not operate as if they were part of a single team playing the same game, or by a set of rules in a predictable manner, where linear cause and effect relationships are easily definable. Further, current challenges and threats transit those boundaries fairly regularly—i.e., human threats, cyber-attacks, and weather events do not pay much attention to either functional or local geographical boundaries.

Since a single CI operator may span a large geographic area, there has recently been increased focus placed on *regional* CI resilience. Various state and local governments need to be able to effectively communicate and coordinate with each other, across jurisdictions. There is a recognized need for both an enhancement of capabilities as well as data-driven analyses that will serve to drive resilience plan-build cycles, especially with an emphasis on cross-sector interdependencies.

To this end, efforts are currently under way to develop an expanded and deepened understanding of regional CI needs and the drivers of regional resilience; improve the definition of regional needs for analyzing, assessing, planning, and improving the cyber resilience and security of regional CI; and increase focus on, and integration of, cyber aspects of resilience at both the federal and regional levels.

CISR Cybersecurity

As supply-chains become ever more specialized and time-sensitive, the opportunity for attacks via that vector increase. For example, there are some medical compounds that rely on chemicals that are only produced in a single domestic facility; others depend on chemicals that have no domestic source. The identification of these critical supply-chain linkages is another area of investigation that is currently emerging in CISR.

It is not clear if EO 13636 intends for the Cybersecurity Framework to address supply chain risks. Often such risks are not addressed in lists of cybersecurity best practices, since assessing these risks requires the examination of manufacturing and shipping processes that lie well beyond the purview of those charged with end-product cybersecurity responsibilities. If supply chain risks to CI are not adequately addressed through the Cybersecurity Framework and its related NIST Special Publication 800-161, then additional steps (Executive or Legislative Branch) might be necessary.

Finally, CI systems are increasingly connected via networks, including the Internet. This connectively, while beneficial from an operational perspective, increases the exposure and vulnerability of these mission-critical systems. As the type and number of cyber-physical systems continue to increase, more, and increasingly advanced, cyber-attacks can be expected on these systems. Executive Order (EO) 13636 is an example of the recognition of this problem. The application of cyber-defensive techniques to CPS, as well as the development of new CPS-specific resilience measures, will continue to be a critical area of R&D.

The need to focus on cross-functional communities is particularly true in the cybersecurity space, in which many CI owners and operators face similar challenges and have the need for similar guidance, information, and assistance. Probes and incursions into CPS are outpacing the capacity of the cyber defenders. These incursions are most likely reconnaissance, and allow adversaries the establishment of a persistent presence from which to prepare for a future attack. Unlike the incidents IT systems experience today, in which adversaries are both learning the terrain and stealing data, Operational Technology (OT) systems seemingly are being "cased." This problem is exacerbated by the convergence of IT and OT types of systems that will be the center of all devices in the future.

Finally, there is the increasing convergence of physical and cyber security. Looking ahead it appears that devices and autonomous platforms will be increasingly interconnected. As more and more devices and platforms are connected, there will be more instances of cyber-attacks that can disrupt and/or threaten the security of CI. For example, the evolution of the Internet of Things (IoT) will provide cyber attackers with additional entry points they could use in physical, cyber, or combined attacks on CI assets.

In summary, the key areas that need to be addressed to ensure that CISR moves ahead are:

- Continued emphasis on developing incentives to allow market forces to effectively drive CISR technology development and adoption.
- Improved analytic capabilities, particularly to identify new attack vectors and quantify cross-sector interdependencies that could result in cascading events.
- Increased focus on developing defenses appropriate for cyber-physical systems and industrial control systems (ICS).
- Considering CISR from a regional perspective.
- Enhancing robust and timely information sharing among government and CI owners/operators taking into account security, business, and privacy concerns.
- Developing new tools to provide improved situational awareness to decision makers in the various sectors during times of crisis, particularly with an eye to cross-sector interdependencies.
- Examining policies, budgets, and regulations at all levels of government to identify ways to increase the rate of CISR technology adoption.
- Focusing on supply-chain vulnerabilities within the various CI sectors to determine weak points, critical linkages, and limiting factors.

Cybersecurity

Introduction

[Note: Since other sections of this paper address Critical Infrastructure Cybersecurity and Resiliency and Identity and Access Management, these topics are not explicitly addressed in this section. Both topics are important parts of cybersecurity.]

Cybersecurity is a broad term used to address all facets of protecting information systems, defending against cyber–attacks, and responding to incidents when they occur. The rapid expansion of information technology with global interconnectivity has led to an enormous rise in cyber–attacks resulting in data breaches, identity theft, cyber–crime, and loss of intellectual property. The world's largest data breaches in recent history are depicted visually at informationisbeautiful.com, where you can see when each attack happened, who was attacked, and the size of the impact. The website contains an interactive version and an excerpt is shown in Figure 14 [45].

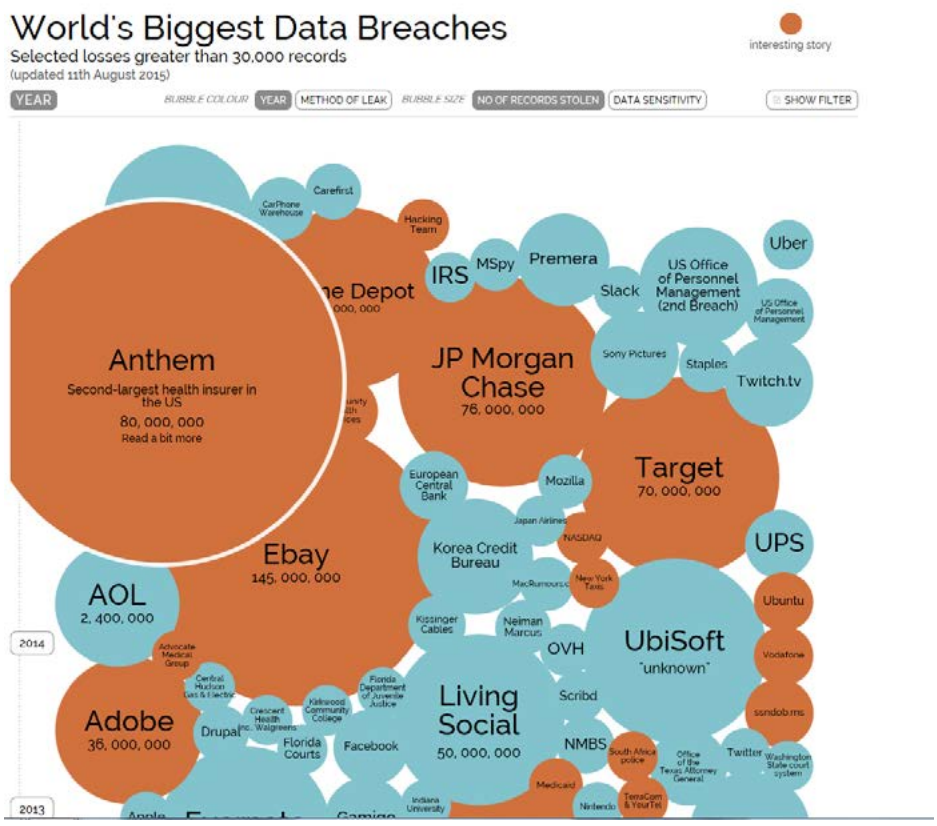

Figure 14. Excerpt of the World's Largest Data Breaches

Cyber–attacks against public and commercial enterprises continue to grow in sophistication. Malware and advanced persistent threat campaigns not only account for frequent serious data breaches and financial and intellectual property theft, they threaten national security. A thriving commercial marketplace has emerged to meet the demand for innovative cybersecurity solutions.

The federal government has responded, as well. In 2011, federal research agencies jointly developed "a strategic plan for cybersecurity R&D that confronts underlying and systemic cyberspace vulnerabilities and takes maximum advantage of the federal government's unique capabilities as a supporter and champion of fundamental research" [46].

A new inter-agency team is in the process of updating the 2011 strategy in response to new federal legislation. In addition to this federal strategy, several agencies (e.g., DoD and DHS) have created and are maintaining agency-specific strategies for guiding their investments in cybersecurity R&D. The agencies' strategies are well coordinated via the Cyber Security Inter-Agency Working Group.

Cybersecurity includes multiple aspects of defense and resilience. There are multiple cyber-security frameworks intended to describe the functions within cybersecurity. One illustrative example of cybersecurity functions is in the NIST Framework for Improving Critical Infra-structure Cybersecurity [NIST Cybersecurity Framework, Version 1.0, NIST, Feb 12, 2014] as seen in Table 6.

Table 6. Multiple Aspects of Cybersecurity

Function	Category
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy
Protect	Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
Detect	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Response Planning Communications Analysis Mitigation Improvements
Recover	Recovery Planning Improvements Communications

Within the cybersecurity community, there is increasing focus on moving from compli-ance with security directives to an approach focused on enterprise risk management and an informed understanding of cyber threats. The landscape of frameworks, guidelines, and commercial services depicts great variety in each one's underlying assumptions about the nature of the cyber threat. There is increasing focus on cybersecurity technologies and ser-vices that can work in the face of cyber threats, including improving the ability to withstand and recover from advanced adversarial threats [47]. A cyber-attack life cycle or cyber-kill chain model, such as the one shown in Figure 15 [48], is helpful in understanding attacker characteristics.

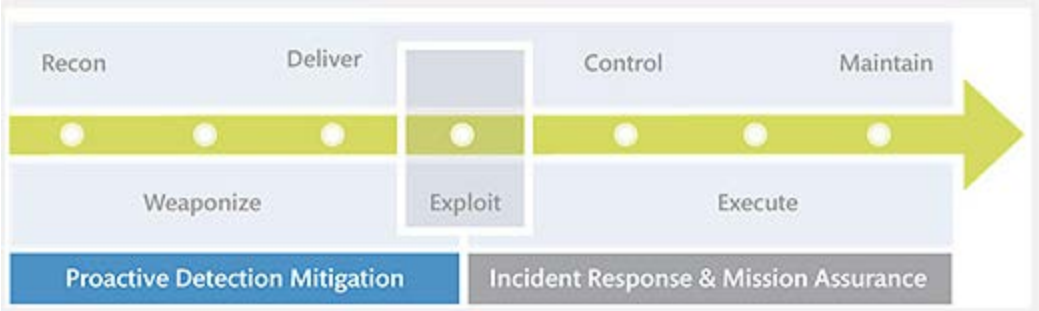

Figure 15. General Cyber Attack Life Cycle Model

Over the past five years, organizations have shifted their focus to add cyber resiliency capabilities, which include systems that can anticipate, continue to operate in the face of, recover from, and evolve to better adapt to advanced cyber threats. Cyber resiliency is based on the assumption that a stealthy, persistent, and sophisticated adversary may have already compromised system components and established a foothold within an organization's systems. As shown in Figure 16, cyber resiliency builds on conventional cybersecurity, security, and continuity of operations.

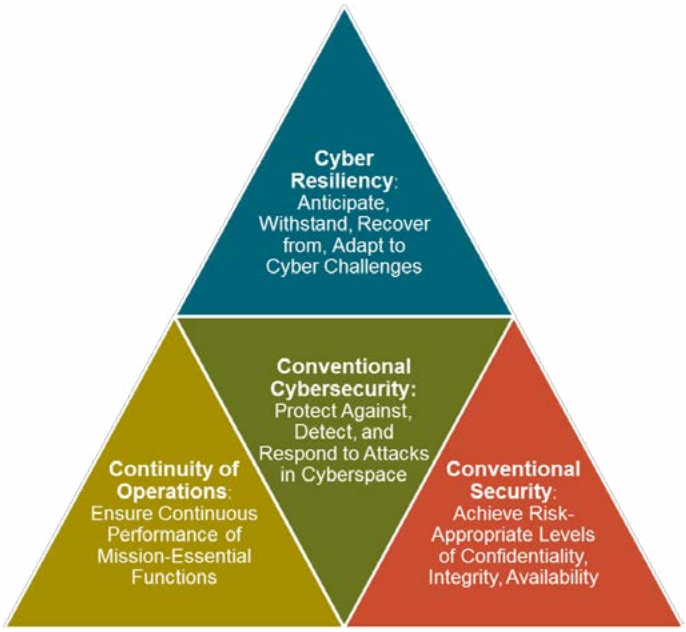

Figure 16. Foundations of Cyber Resiliency [49]

Landscapes

Global Landscape

According to Gartner, the global cybersecurity market has grown from $67B in 2013 to $76.9B in 2015 and is expected to grow to $93B in 2017 [50]. The largest cybersecurity markets—North America, Asia Pacific, and Western Europe—have a cumulative market share

exceeding 50 percent. Network security, data security, and identity and access are the three largest cybersecurity segments in most countries, with the data loss prevention segment recording the fastest growth at 18.9 percent. This market depiction probably underestimates the commercial investments in cyber through corporate R&D, for which data is not always available.

Regulatory compliance has become a major factor driving increased spending, with regulatory pressure growing quickly in Asia Pacific and Western Europe. Examples include the Australian Privacy Act, China's guidelines regarding personal information protection, additions to the E.U. Data Protection Directive, and personal data protection laws in Singapore and Malaysia.

Leading international cybersecurity companies include Airbus Defense & Space (EADS Group, France), Finmeccanica SpA (Selex SE, Italy), Kaspersky Lab (Russia), QinetiQ (U.K.), Thales Group (France), and Trend Micro (Japan).

For mobile devices, most R&D investment is found in the United States (Google and Apple) and South Korea (Samsung). China and Japan are also leaders in communications but they seem to be imitating or integrating innovations that come from the United States and/or South Korean giants. China dominates the manufacturing of smartphones, which means they control most of the supply chain. China also possesses most of the firmware and Original Equipment Manufacturer (OEM) "stock" builds supplied by the tier one giants.

National Landscape

Industry Landscape

The U.S. federal cybersecurity market is valued at $65.5B cumulatively over five years (2015–2020) [51]. According to the Networking and Information Technology Research and Development (NITRD) Program, it is the nation's primary source of federally funded work on advanced information technologies in computing, networking, and software [52]. NITRD's cybersecurity and information assurance R&D investments totaled ~$800M, or about 20 percent of its overall budget across NSF, DoD, DARPA, DOE, NIST, and DHS. Some of these investments are for developing scientific foundations (both science of security and cross-cutting foundations), maximizing research impact (supporting national priorities), and accelerating transition to practice. The remaining investments are directed toward inducing change in four areas: Tailored Trustworthy Spaces, Moving Target Defense, Cyber Economic Incentives, and Designed-In Security.

The U.S. cybersecurity industry has received $5.2B in investments during the past five years. According to CB Insights, venture capital firms alone invested $1.4B in 2013 and $894M in the first half of 2014; and this upward trend is expected to continue in 2015. Booz Allen Hamilton, Science Applications International Corporation (SAIC), and Northrop Grumman were the top three contractors in defense cybersecurity, while Dell, Hewlett-Packard (HP), and Computer Sciences Corporation (CSC) were the top three cybersecurity providers to civilian agencies [53]. The merger and acquisition market is also heating up, e.g., Google,

McAfee, and Symantec acquired eight companies each in the cybersecurity space during 2014.

Gartner identifies cybersecurity market leaders as companies that have both vision and excellent execution. To keep up with this rapidly evolving market, the top players are likely making heavy investments in R&D. Gartner has segmented cybersecurity products into the major categories listed in Table 6. The network security segment dominates the market with a share of 35.1 percent, with data security (28.4 percent) and identity and access (19.4 percent) as the next biggest segments. The cloud security market is growing at a healthy pace. Mobile security is not a top priority at present but is expected to grow after 2017.

The cybersecurity industry is evolving at a frenetic pace. In 2002, there were only five leaders in cybersecurity. Today, many new leaders are emerging, such as FireEye and Palo Alto Networks, and they are being acquired by larger companies seeking to offer one-stop integrated platforms rather than point solutions.

A key differentiator for companies in the cybersecurity space is access to robust cyber threat information. For example, companies such as Mandiant are intimately involved in helping companies recover after major Advanced Persistent Threat (APT) attacks and have built robust threat intelligence capabilities and databases. Awareness and knowledge of the real threat enables innovators to build cybersecurity capabilities that have impact on adversaries.

The cybersecurity needs of CPS are also driving innovation, as there are few existing solutions that effectively protect OT, compared to IT. Enterprise IT is focused primarily on integrating and streamlining business practices, while OT is focused on managing industrial processes. In 2014, Lockheed Martin acquired a cybersecurity company called Industrial Defender that is widely recognized as a leader in securing the control systems managing critical industrial infrastructure. Other leaders in this space include IBM, Siemens, Dell/Secureworks, McAfee, and Symantec.

Another key trend in industry is protecting managed security services; according to Gartner: "By 2018, more than half of organizations will use security services firms that specialize in data protection, security risk management and security infrastructure management to enhance their security postures" [54]. This trend is driven by two primary factors. First, many organizations lack the sophisticated cybersecurity skills needed to define, implement, and operate effective security controls, so they must hire security consulting firms specializing in the needed skills. Second, there is a clear movement away from a protection paradigm toward a detect-and-respond paradigm, which has resulted in significant growth of managed security services that specialize in mitigation and incident response.

Government Landscape

Following high-profile cybersecurity incidents and data breaches of private and government systems, the Federal Chief Information Officer (CIO) initiated a government-wide 30-day Federal Cybersecurity Sprint during July 2015, followed by a Cybersecurity Action Plan. Office

of Personnel Management and an interagency team from the DoD, DHS, and the Federal Bureau of Investigation (FBI) "identified 15 new steps to improve security and modernize its systems including completing deployment of two-factor strong authentication for all users and expanding continuous monitoring of its systems." [www.opm.gov/cybersecurity] The Cybersecurity Action Plan also includes automated sharing of cyber-threat indicators, accelerated deployment of Continuous Diagnostics & Mitigations, a reduction in the number of and improving security associated with Internet connections from government systems.

In 2012, National Cybersecurity Center of Excellence (NCCoE) was established at NIST to focus on improving commercial offerings in cybersecurity suited to industry sectors and government systems. NCCoE aims to address businesses' priority cybersecurity problems with standards-based solutions using commercially available technologies. Its approach is to forge collaborative relationships with experts from industry, government, and academia to reduce the barriers to adoption of secure technologies. They aim to do this by integrating available technologies into end-to-end solutions that can be applied to industry use cases.

Academic Landscape

A decade ago there were just a handful of universities that were recognized academic centers of gravity in cybersecurity. The explosive demand for cybersecurity solutions has resulted in vibrant research activities at numerous academic institutions across the country. No clear leader from academia has emerged and, according to a survey of top security conferences, no clear centers of gravity have yet emerged. Rather, the research landscape has become fragmented. Also, for the most part, academia has taken on the role of a fast follower in many areas (e.g., mobile security) focusing primarily on incremental innovations.

Looking Forward

Cybersecurity is a continually evolving problem with innumerable challenges to be addressed. There is still a need for strong cybersecurity foundations, especially with the expectation that quantum computing will become a reality within a few decades. At the same time, new challenge areas are emerging as potential priorities, such as cyber deterrence, mission assurance, adaptive security, and CPS security. In addition, some technologies (e.g., identity, authentication, and access management) are being re-examined in light of the increasing momentum and scale of the Internet of Things.

The rapid pace of innovation has prompted DoD and DHS to establish offices in Silicon Valley to develop deep public-private partnerships, both to transition technologies developed by government and national labs, and to leverage technologies developed by industry. Indeed, a whole-of-nation approach is essential to tackling the vast challenges of cybersecurity.

Improved Response to Cyber Attack Life Cycle

The Attack Life Cycle in Figure 15 shows the steps in a typical cyber-attack. Looking forward, researchers from various organizations are working on ways to improve our ability to deal with cyber-attacks—including efforts to more effectively identify indicators "left of exploit,"

that is, before an exploit occurs, and efforts to improve efficacy of response "right of exploit" through more timely detection of cyber intrusions. Organizations are moving to a threat-focused orientation. This involves sharing actionable threat information among the constituent parts of an organization's enterprises systems, as well as among different organizations. Some threat-sharing groups are based on industry sector or geographic regions.

Organizations also need improved digital forensics tools and techniques, which provide the analysis of digital media, data, devices, and/or network data used for specific circumstances, such as in a court of law. Digital forensics tools and techniques also support cyber threat analysis, malware analysis, and incident response. Enhanced techniques and improvements in digital forensics are expected to improve the ability to detect malicious behavior, especially for newer technologies such as mobile, embedded systems, Internet of Things, and distributed cloud services.

Cyber Threat Information Sharing

Organizations within government, industry, and academia all need to increase their efforts to share data on cyber-threats so that they can better understand and respond to the external threat environment. Sharing threat information is an important element in enabling effective collaboration. In the last several years, government and industry leaders have emphasized the importance of information sharing. However, sharing information is just a means to an end—the goal is to make use of the information so that organizations can:

- Tailor their defenses based on threat information they receive.
- Analyze the information they receive and provide new insights to themselves and others.

For example, suppose Company A and Company B have agreed to share cyber threat information (see Figure 17). Company A identifies an attacker trying to gain a foothold in its network. It shares this information with Company B, which loads this new information into its sensors to see if it can detect the threat. Company B sees the threat and analyzes it, discovering new information about the attacker. Based on these new insights, Company B again tailors its sensors. Company B also shares the new information with Company A, which tailors its sensors accordingly, and Company B shares this information with other collaborating organizations. In this hypothetical case, Company A and Company B not only tailored their defenses based on shared information, they also gained new insights that enabled them to go beyond what they could have achieved independently.

While hypothetical, this scenario describes sensing, analytical, and information sharing capabilities that exist today.

Figure 17. Hypothetical Cyber Threat–Sharing Scenario

To support these efforts, DHS has been leading a collaborative effort with industry to develop a comprehensive language for automated threat–information sharing and collaboration. That language, called Structured Threat Information eXpression (STIX), can carry an extensive set of cyber–threat information that characterizes the cyber adversary's motivations, capabilities, and activities. DHS also supported the development of a secure and automated mechanism to transport threat information from one organization to another, called the Trusted Automated Exchange of Indicator Information (TAXII). TAXII is a set of services and message exchanges that enables sharing of actionable cyber threat information across organization and product/service boundaries.

Organizations also need tools to understand the information they are sharing so they can use it to adjust their defenses and modify their procedures. They also need tools to extract threat information from their own sensor data to understand it and then share that information with others who have agreed to participate in information sharing.

Cyber Resiliency

To the extent possible, organizations want to prevent attackers from compromising their data and systems. Knowing that this is not always possible, organizations are adding more cyber resiliency capabilities to their cyber frameworks. This includes the ability of cyber systems and cyber–dependent businesses and missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats.

Cyber resiliency is based on the assumption that a stealthy, persistent, and sophisticated adversary may have already compromised system components and established a foothold within an organization's systems. As organizations become more threat-aware, cyber resiliency is expected to play a larger role in an organization's approach to improve its cybersecurity posture. In the future, we expect cyber resiliency techniques to mature and become valuable tools in an organization's toolkit to address advanced cyber adversaries.

Cyber resiliency techniques are intended to affect adversary activities across the cyber–attack life cycle.

Table 7. Potential Effects of Cyber Resiliency Techniques on Adversary Activities Across the Cyber Attack Life Cycle

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	Contain Curtail		Negate Curtail	Negate	Degrade Delay Contain Curtail	Negate Curtail Degrade Delay Recover	Degrade Delay Con- tain Curtail
Analytic Monitoring	Detect Analyze		Detect Analyze	Analyze	Detect Analyze	Detect Analyze	Detect Analyze
Coordinated Defense		Delay		Degrade Delay	Detect Degrade Delay	Degrade Delay	Detect Degrade Delay
Deception	Degrade Delay Divert Deceive Detect Analyze	Deter Deceive	Deter Divert Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive De- tect Analyze	Deter Divert Deceive De- grade Detect Analyze	Deter Divert Deceive Detect Analyze
Diversity	Degrade Delay	Degrade Delay	Degrade Delay Contain	Degrade Negate	Degrade Contain Recover	Degrade Recover	Degrade Contain Recover
Dynamic Positioning	Detect Curtail		Negate Divert		Detect Degrade Delay Curtail Expunge Recover	Degrade Delay Curtail Expunge Recover	Detect Degrade Delay Curtail Expunge Recover
Dynamic Representation	Analyze				Detect Analyze	Detect Recover	Detect Analyze
Non-Persistence	Degrade Delay		Negate	Curtail Expunge	Curtail Expunge	Curtail	Curtail Expunge
Privilege Restriction	Degrade Delay			Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain
Realignment	Degrade Delay	Negate Degrade Delay	Negate Degrade Delay	Degrade Delay	Negate Degrade	Negate Degrade	Negate Degrade
Redundancy						Degrade Curtail Recover	
Segmentation/ Isolation	Contain		Degrade	Contain	Degrade Delay Contain	Degrade Delay Contain Recover	Degrade Delay Contain
Substantiated Integrity			Negate Detect		Detect Curtail	Curtail Recover	Detect Curtail
Unpredictability	Delay	Delay	Detect	Delay	Delay Detect	Delay Detect	Detect

As stated earlier, organizations from industry, academia and government must continue to work together to battle cyber-attacks. Together, their innovations are expected to lead to more mature cyber resiliency techniques that can be applied in the future.

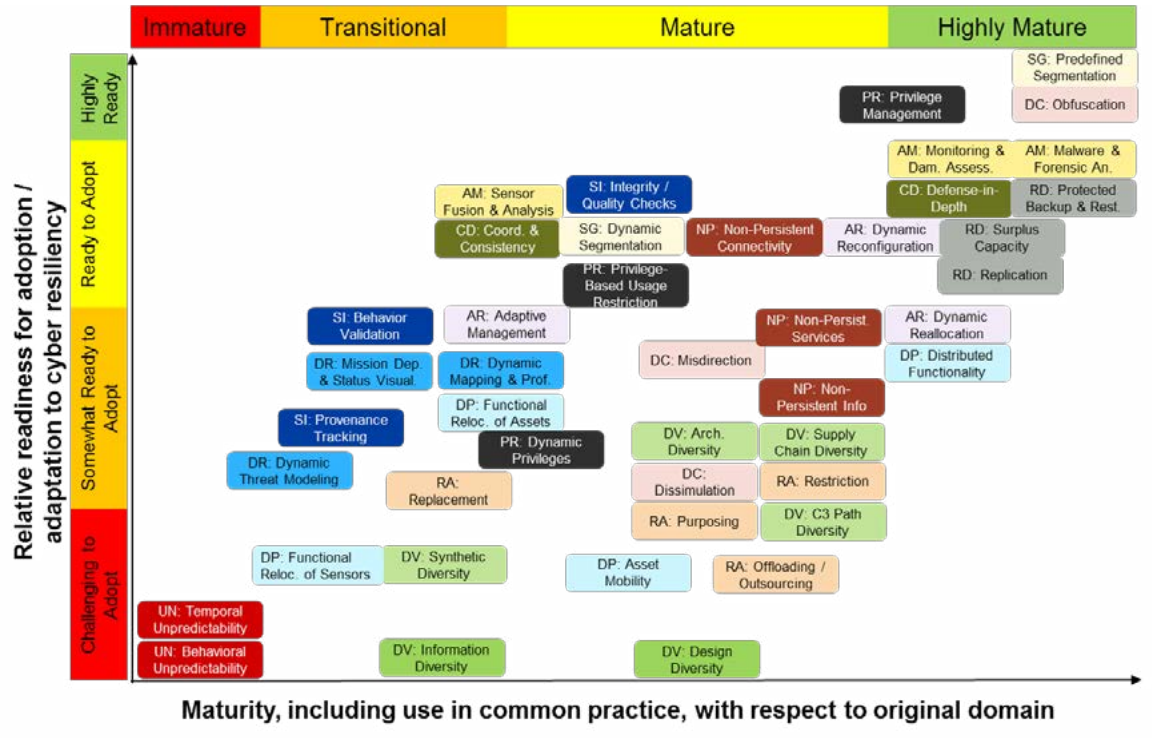

Figure 18. Relative Maturity and Ease of Adoption for Approaches to Implementing Cyber Resiliency Techniques

Technologies

Data Analytics

Introduction

Data analytics is a broad area—encompassing data science, big data, statistical processing, decision aids, and machine learning—which is focused on providing a "decision advantage" for an organization. Its overall purpose is to improve decision-making capabilities in many different domains.

The term "big data" tries to capture the huge amount of information humans are receiving today—including the *volume* of information, the speed (*velocity*) of information arriving, and the *variety* of information (text, images, video), all and any of which might be critical to our decisions. These three Vs as they are called have been shown to be beyond the capabilities of many current fourth-generation data management and computing technologies. In response, organizations are seeking new technologies to handle the kinds of problems that require more information than people are able to analyze and understand in a timely manner.

More fundamentally, big data scientists are challenging classic scientific methodologies within the field of data analytics around how to best use data to make decisions. The new

approach, in which users "let the data expose the patterns," is in opposition to classic methodology in which users first form a hypothesis and then examine data from experiments to test the hypothesis. It may be the case that today some cause-and-effect relationships are so complex that we have to rely on computers to find the patterns because, while individual human brains are computationally exceptional, we simply cannot ingest the critical data for a complex decision.

Big data is big news for a reason. The transformational change it has promulgated can be measured by dramatic increases in efficiency (of resource utilization and cost avoidance), effectiveness (of outcomes), timeliness, and/or accuracy of decisions. The value of improved information accuracy and timely situational awareness can be counted in lives saved, costs avoided, or fraud detected.

Numerous technologies support data analytics, from developing data-analysis algorithms to fusing and visualizing complex data so it can be quickly understood and acted on. Thus, there are many opportunities to advance data analytics. The data itself varies from thousands of hours of video to millions of social media messages to millions of tax returns.

Data analytics advancements will rely on a number of critical global and national investments and partnerships among research centers, academia, and industry. These advancements should move many of our national decision-making challenges to a new era in which "gut feeling" and past experience isn't the only driving methodology. If data analytics continues to expand in use and capability over the next few years, we should be able to more accurately drive our decision processes based on factual current data and predictive models of outcomes and options or alternative courses of action.

Industry is already using these advanced technologies for purposes such as credit card fraud detection. In coming years, they will use them for activities such as personalized healthcare analytics, strategic long-term investment decisions, and government program resource optimization.

One challenge to advancement includes the development of the fundamental analytics layers of such systems. Most practitioners would agree that data analytics that inform real-world decisions need five key layers in a repetitive cycle: data acquisition, preparation and pattern recognition, information management, visualization and presentation, and decision support.

Landscapes

Global Landscape

Global investment in data analytics varies by regions. For example, there appears to be more doubt about big data's value in the United States and Canada than in most countries. It may be that developing nations and economies are looking more aggressively at ways to capture markets, while U.S. and Canadian companies are considering the needs of the over-marketed and technology-savvy North American consumers.

Research centers have been investing for years in a complete approach that includes exploitation of data as well as data presentation and option awareness concepts. Researchers are striving to show users that with the right data they can make better and more-timely decisions than if they rely solely on their intuition and experience. However, the data-driven decision dilemma highlights the fact that advancing data analytics requires behavioral changes as well technological changes.

Companies around the globe are investing to various degrees in improving data analytics capabilities and technologies. Figure 19 shows the Median Expected Spending Per Company on Data Analytics in 2015 by country. By the end of 2015, companies across the surveyed regions expect to spend 75 percent more on data analytics efforts, with Australia and the U.K. projecting the highest spending per company. Median spending across all countries is projected to increase by 75 percent to $17.5M on average in 2015.

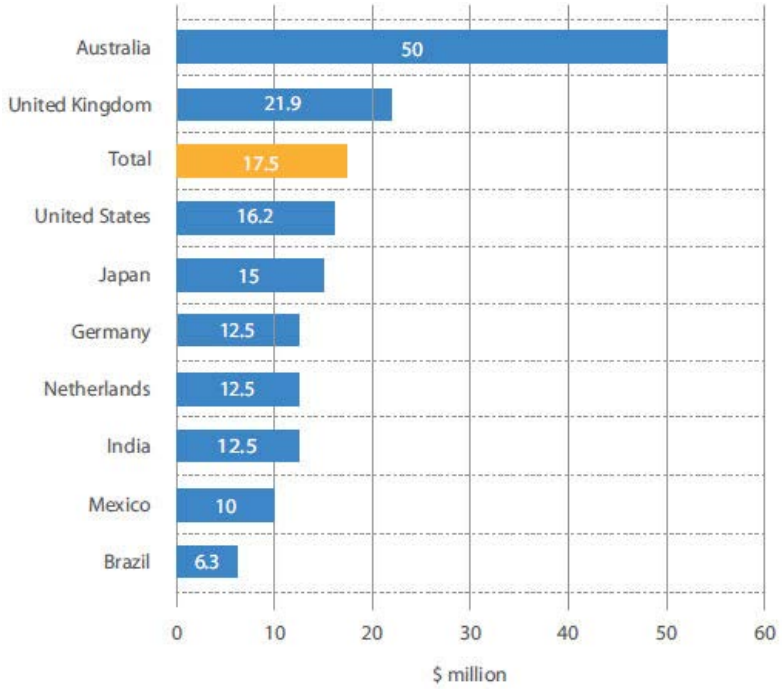

Figure 19. 2015 Median Global Corporate Investments by Country in Key Analytics Technologies [56]

Figure 20 notes that global investment in four of the major big data technology areas (analytics, cloud services, mobile analytics, social analytics) appears to be stabilizing in terms of the number of organizations continuing to invest in these areas, although there are notable decreases in Spain and increased investment in both China and India. The median investment globally (not depicting the size or scale of investment) shows that two-thirds of all organizations are deploying and plan to continue to deploy solutions with these key technologies.

Enterprises deploying each technology

	Big Data & Analytics	Cloud	Mobile	Social
Worldwide	75%	75%	78%	70%
US	82%	83%	82%	79%
Mexico	78%	65%	74%	69%
UK	77%	77%	79%	72%
France	80%	76%	80%	68%
Germany	62%	73%	75%	59%
Italy	79%	73%	69%	67%
Spain	76%	72%	82%	71%
Japan	48%	54%	50%	44%
Brazil	79%	84%	90%	73%
Russia	76%	63%	71%	45%
India	82%	79%	82%	74%
China	81%	80%	90%	85%
S.Africa	70%	60%	70%	71%

Enterprises increasing investment over next two years

	Big Data & Analytics	Cloud	Mobile	Social
Worldwide	76%	75%	77%	66%
US	81%	75%	77%	66%
Mexico	67%	70%	74%	59%
UK	74%	79%	74%	69%
France	62%	73%	76%	68%
Germany	63%	69%	71%	56%
Italy	73%	75%	76%	65%
Spain	54%	67%	64%	56%
Japan	54%	49%	52%	39%
Brazil	69%	86%	77%	73%
Russia	72%	70%	71%	47%
India	85%	90%	86%	78%
China	90%	87%	86%	80%
S.Africa	76%	74%	79%	74%

Figure 20. 2015 Global Adoption of Big Data Technologies by Country [57]

Looking forward, Figure 21 depicts the economic investment in specific data science areas projected into the future. This diagram shows that data analytics will remain dominant in the consumer business intelligence domain. (Note: it is unlikely government uses of this technology area were well covered in this kind of public survey.)

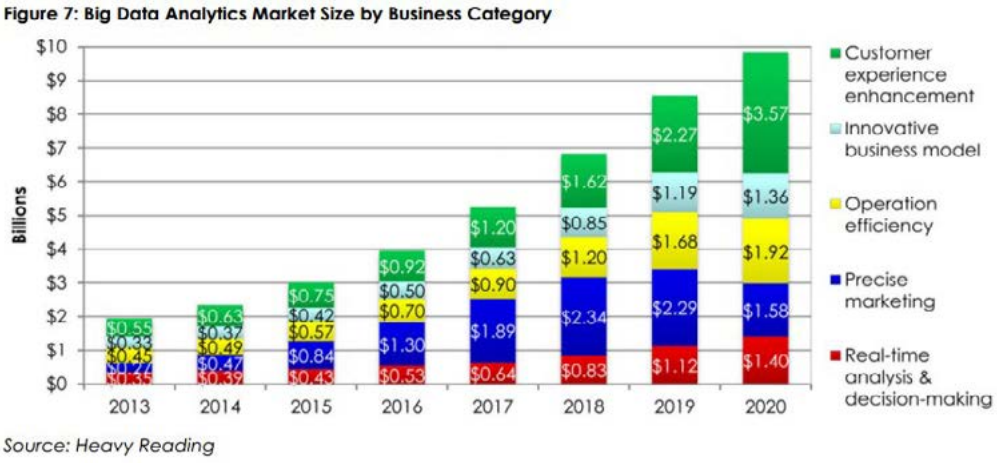

Figure 21. Data Science Analytics Investment by Business Category [58]

National Landscape

There are various ways to describe and cluster key U.S. investments related to analytics technology investment areas. One is by technology: big data, machine learning, visualization, and decision support. Another is by domain mission area, including intelligent cities, fraud and financial stability, and healthcare. Overall data analytics investment continues to rise and this momentum is projected to continue for the next several years, as shown in Figure 22.

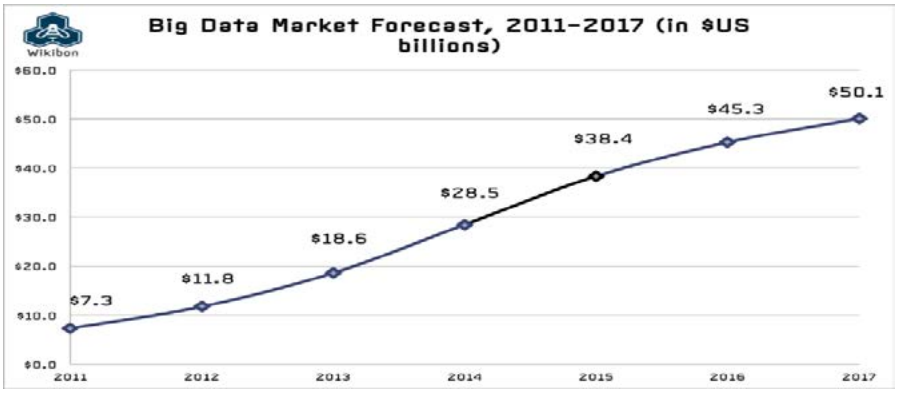

Figure 22. U.S. Data Analytics Market Size [59]

Industry Landscape

The wide variety of vendors reflects the variety of technologies supporting data analytics, many of which are offering packages of capabilities and services. Cloud service providers are a natural pathway to the hosting of data analytics for many companies today. While individual analytics tool or engine providers supply the hands-on tools, cloud service providers supply the workshops and physical infrastructure for many organizations today.

While some companies still host and run their own data centers, the popularity of and trust in large data center providers appears to be increasing. Figure 23 shows that Amazon is the leading cloud service provider, with many competitors fighting to be in the top three. Docker is currently in second place, having quickly risen from almost non-existence. Third is Cloudera, the leading HADOOP vendor, which provides key underlying software services that run above the physical infrastructure provider offerings and below the actual analytics tool applications.

Some companies, such as Microsoft, IBM, and Google have "verticalized" their offerings to provide all levels of needed facilities/hosting, services, middleware, and data analytics tools. This technology allows the packaging of analytics modules for rapid creation in any mission center. OpenStack is also moving up quickly, along with HortonWorks.

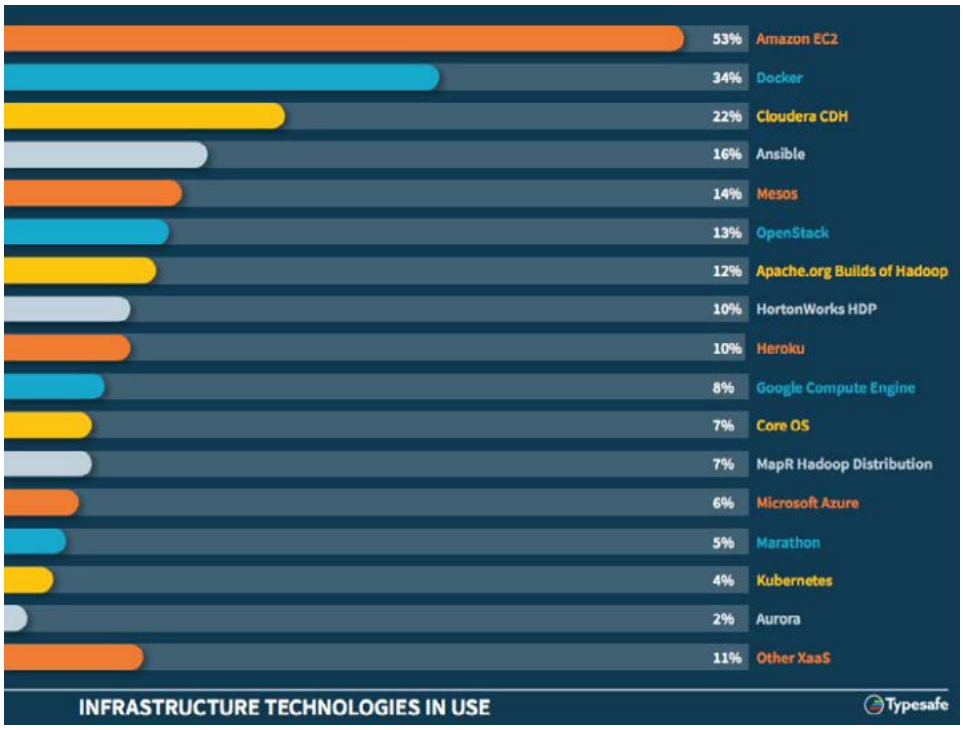

Figure 23. Leading Cloud Infrastructure Vendors [60]

Gartner assesses business intelligence (BI) vendors in a quadrant chart (Figure 24) that measures value or successful use on the y-axis and long-term planned continued use on the x-axis. Vendors want to be in the upper left quadrant as an orange dot denotes a more likely to be used future product.

What this kind of analysis doesn't show, however, is the smaller and unexpected analytics innovations of which there are potentially thousands. Some are niche-specific, some reusable across domains, and some composite "threads" of many individual vendor, government off-the-shelf (GOTS), open source individual components or analytics. In some research centers, teams have structured their major investments into mission threads, chaining together many COTS, GOTS, open source or in-house developed components. Such hybrid combinations of products would not likely show up in any market study, as the studies are not looking at a specific mission context to determine value.

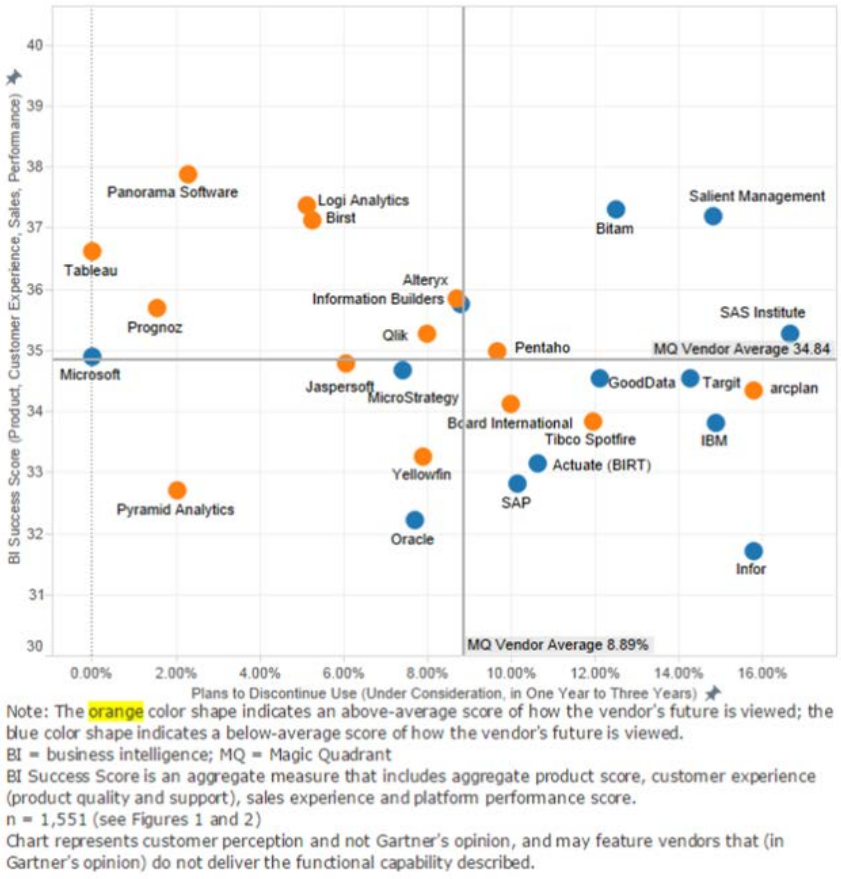

Figure 24. Gartner Magic Quadrant of Business Intelligence (BI) Vendors in 2014

Looking Forward

There are many data analytics challenges—some fundamental long-term problems—yet to be solved, providing opportunities for government, academia, and industry to make analytics as effective as they can be. This section describes many of the technical challenges as well as the policy implications to be addressed in data visualization, mobile data, cloud services, and automated and predictive analytics.

Data Visualization

In the mid-1990s, the rise of e-mail made the Internet more accessible to consumers and drove user adoption. Similarly, data visualization tools will make data analytics more accessible in coming years. Visual analytics (also called data discovery or data exploration) allows users to ask interactive questions of their prepared data sets and get immediate responses in a visual format that makes the whole process engaging and understandable. This capability will democratize access to data and foster a strong data-analysis culture in which business users will look for data and perform visual analyses before making decisions.

There are dangers, however, in the democratization of data. Before government leaders make decisions based on colorful new visualizations, they need to be positive their data

is accurate and their tools are built on decision science principles, which is not a given for today's systems. The majority of people today believe what they read on the Internet, and they are very likely to believe and make decisions based on real-time visualizations that come from drop-down menus in exciting graphic tools. Quick visualizations do not guarantee accurate decision making.

Another example is the popular use of social voting (e.g., "likes" and "dislikes) to assess a service or product. Users need to be aware of the value of the data they are using to make decisions. Here again, changing behavior is as important as building technology.

Mobile Data and Data Motion

Smartphones and tablets have fundamentally changed consumer habits. Mobile video is the fastest growing segment of mobile data traffic. Organizations need to think strategically about engaging with citizens/consumers on their mobile devices. The mobile Internet is predicted to take over desktop Internet usage; in fact, some studies say it already has. According to Groupe Speciale Mobile Association (GSMA), consumer monthly spending on mobile content and services in emerging markets has reached almost $1B, which presents an additional significant marketing and data analytics opportunity.

The top priorities for companies will be defining mobile metrics that matter, understanding mobile technology and the data creation process, and collecting and analyzing mobile data. Challenges include addressing security and privacy concerns.

Adoption of Cloud Services

Cloud computing platforms, such as Amazon Web Services and Microsoft Azure, will continue to gain ground in coming years. Of course, organizations should understand how to use these platforms, as well as the risks, before they make critical decisions.

Big data analytics solutions that require a pay-as-you-go data storage and computing-intensive analysis infrastructure can leverage these platforms and go to market with much lower capital costs than ever before. Innovations, such as the cloud data warehouse platform from Amazon's RedShift, will gain ground and set new standards in self-service business intelligence, which will enable scalable, fast, and secure solutions at affordable prices. The robustness of this platform will allow organizations to save on infrastructure design, set up, and management costs. It will free them up to focus on issues that matter most for their customers and focus on gaining and acting on business insights.

Predictive Analytics

For many years, companies have built data platforms and analytics infrastructure with a significant emphasis on hindsight—that is, look-back reports that help businesses check their rear-view mirrors. However, enterprises are beginning to see the value of looking ahead and using data for insights, predictions, and foresights. With better insights and a forward-looking predictive views, organizations are hoping to be more proactive. For example, CIOs are thinking about their predictive analytics needs as they build today's infrastructure

and explore newer technologies, such as Hadoop, to manage their unstructured data and co-exist with their traditional data stores.

Predictive analytics will significantly gain ground in the coming years, supported by the quick wins in data visualization and the increasing appetite to explore data for decision making. An even more important contributor, however, is machine learning (ML), which has exploded in the past five years. Like data visualization, this kind of technology requires very skilled data scientists and computational scientists to use effectively. Google's internal Brain project is apparently trying to reuse well-built ML components so that others in business-specific roles can leverage them. However, the quality and accuracy of chaining these components together into analytics systems and continuously revalidating the accuracy and precision of these systems is a challenge. Another challenge is just finding the skilled staff to develop and operate these complex technologies in a limited talent pool.

Support for Future Data Analytic Innovation

In addition to the technology innovations and challenges being addressed today, there are some higher order national policy issues that need to be addressed in the future. These include the following.

Privacy in Intelligent Cities

How could the aggregate of all the data coming from thousands of sensors deployed by government organizations, commercial companies, and the public (e.g., on mobile devices) be used or abused? For example, combining New York City's taxi pick-up and drop-off data sets with location data, which are published openly, could offer embarrassing insights into where specific people were picked up and dropped off. This is an open use of public data, but it could be employed to damage people's lives. While "opt in policies" have been developed to prevent this kind of use, it would be naïve to think that these will solve privacy issues.

Today, DoD and Intelligence Community (IC) organizations, as well as market intelligence teams and political survey teams, use pattern of life analytics around the world. In fact, people can't easily hide their patterns of behavior. The challenge for government and industry is to balance the art of what is possible with the need to meet the public's expectation of privacy protection. In addition, these behavioral pattern recognition techniques need to be expanded to many other federal government issues to further optimize federal resources and maximize societal gains.

In conducting extensive reviews of privacy policy, MITRE researchers were surprised at the amount and types of data that can be purchased by anyone or is publically derivable, including the details of private contract offers and global company intelligence.

The topic of privacy in a world of sensors will get more and more heated. Today we are in the Wild West and privacy is the victim often left behind. Government and industry need to develop clear, resilient guidelines for private and public use of data.

Ensuring Competition in Analytics Systems

Another challenge is how to ensure real competition in analytics system development, an area dominated by well-supported but highly proprietary vendor solutions. To offer an alternative, some organizations have created open source analytics frameworks (such as Unstructured Information Management Architecture, originally from IBM, or Mahout for machine learning) to keep competition alive in the analytics development world.

Many researchers and analytics developers don't want to buy into the big, established frameworks for analytics—despite their capabilities—because they lock you in long term once your analytics are integrated into their framework. For example, some cloud service providers lock your data in once it is on their system through their pricing models for data movement.

Government and industry need to find the best way to address this tension. The large companies in this space, including cloud service providers, have developed powerful and complete solutions; however, many in the developer community are hesitant to tie themselves to one vendor for fear of competition limitations in the future. These developers believe frameworks that integrate component analytics into larger valuable analytics threads must be open and not proprietary.

This is a lesson many government organizations have already learned. The commercial vendor approach, which offers agile and quick solutions, is often the preferred short-term solution, despite the proprietary framework. How can government ensure open competition yet still take advantage of valuable commercial solutions?

Budgeting Requirements for Data Analytics Systems

Investing in data analytics systems requires knowledge of how they work, including the long-term costs. Government financial and acquisition policy are not yet in sync with the requirements of building complex learning systems.

For instance, in many analytics programs, the cost of continuous tuning of the analytic threads to new and changing data over time isn't budgeted into the long-term plans. In addition, when the government builds any kind of analytics system, the initial rules/patterns that are used for acceptance tests are often based on historic use cases. When users input new scenarios (such as new fraud schemes), the systems may fail because they were trained to recognize past patterns of behavior. In creating budgets for these systems, organizations must include continuous improvement (or "tuning") of the system's machine learning capabilities. Without budgeting for continuous quality improvement, organizations will never reap the benefits of their investment.

Identity Management in a Virtual World

Introduction

The act of establishing an individual's identity and subsequently using that identity for a range of government, civil, or personal purposes requires a family of technical tasks that have become both increasingly important and increasingly difficult. They occur against a backdrop of improved technical capabilities (e.g., better face recognition), and a proliferation of digital media, interconnected mobile devices, and information security challenges for individuals as well as local, state, and federal governments.

Identities can be thought of as cyber or physical.

- *A cyber identity* is a construct comprising multiple factors or attributes such as name, residential address, email address, phone number, etc. The accuracy of these attributes may or may not be validated through cross checks via credit reports or other means. There is an association of a cyber identity with a virtual actor accessing services online. Most people have multiple cyber identities, each of which has very different purposes. For example, the same person/actor may use different identities to: use a credit card to order pizza online, apply reward card points when purchasing groceries, and file income taxes electronically.
- *A physical identity* is also a construct comprising multiple attributes (e.g., name, fingerprint, eye color). The accuracy of these attributes also requires validation, and there is a direct association of a physical identity with a physical actor. What isn't as immediately obvious is that an actor also has multiple physical identities, based on the role of the identity. For example, the same actor can be a mother, a coach of a soccer team, and an employee at a security firm. The first is generally accepted de facto but can be verified via a DNA test. The second will require a background check to ensure this actor is not a pedophile (yet another identity). The third would require a background check and then a badge and other potential identifiers such as personal identification numbers (PINs) to gain access to corporate systems.

What is clear is that the successful management of these identities, whether the information is collected from or offered by the actor, requires an increasingly complex ecosystem. It is not an exaggeration to suggest that this successful management is an issue of critical national importance. All of their identities provide people with a seamless entrée into a world that allows them to communicate with each other, interact with their government, conduct commerce, and access health services in ways not possible just a generation ago. If, however, these identification systems fail, the underlying fabric of our society will fray and tear, causing disruptions not imagined a generation ago.

Identity itself is fundamentally established in terms of *what you know*, *what you have,* and *who you are*. *What you know* refers to passwords, personal identity numbers, and various security questions that imposters would not likely know. *What you have* refers to tokens, previously issued identification badges, licenses, or credentials. And *who you are* refers to biometric traits you possess that are robust and stable enough for authentication or strong

identification. For example, a single fingerprint can be used for authentication to verify who you claim to be (1 to 1 matching), and ten fingerprints can be used to determine who you are or if you have been previously encountered (1 to N matching).

Identity *management* is simplest when all the individuals involved are members of a unitary community; complexity arises when community boundaries are porous, ambiguous, or non-existent. Identity approaches that rely on databases are themselves most reliable when the integrity of those databases is above reproach. In this period of frequent data breaches, however, this can no longer be taken for granted.

Identity *proofing* is the process of verifying that a person is who they say they are when they enroll or otherwise create an identity for a system or service. Depending on the level of assurance required by the system or service, this can be as simple as an assertion by the person (e.g., Facebook just requires a name, birthdate and either a valid email or mobile number) or so complex that it requires a valid birth certificate or passport as well as a full background investigation (e.g., acquiring a government clearance).

Identity *protection* is designed to provide privacy. Discretion and safeguards are applied to prevent disclosure of identities or personal information to the general public or to unauthorized or adversarial uses. Common examples include credit card and bank account information, as well as personal medical and insurance records. Other identity protection needs involve the protection of minors and witness protection programs.

At its essence, the problem of identity is the problem of establishing and maintaining a set of attributes that, in some combination, can be used to confirm that a given person is who he says he is, or who we think he is. For any such scheme to work, some of the attributes must be stored and then used in verification functions or *authentication factors* against each presented or claimed identity.

At the inception of the digital age, a simple userid and password combination was considered sufficient to authenticate a person. It wasn't long before bad actors began cracking the passwords (first by brute force and then via more sophisticated attacks). Other authentication techniques include secret, shared questions, one-time passcode generators, and "out of wallet" questions. Correspondingly, attackers have found ways (such as large-scale identity data thefts) to foil these techniques. Today, multi-factor authentication techniques and out-of-band communications are increasingly used more. Only time will tell when (and not if) these methods will be circumvented and new techniques will need to be employed.

The use of innate physiological or behavior characteristics—biometrics—are helpful in identifying a person who is physically present, but even these attributes have been spoofed. The rise of ubiquitous information systems and computer networks, permeating the fabric of government and the larger society—the Virtual World—has introduced new tasks, new challenges, new threats, and new opportunities.

Landscapes

Current identification systems are mainly used for enforcement purposes and for situations in which the government collection of identity information is a necessary part of the process. Increasingly, we have the capability to identify, track, and locate individuals through data generated by social media and personal health or lifestyle devices and applications. The collision between personal communications and conveniences and unwanted or unintended identification is a contested area in which policy, enforcement, and recovery procedures lag significantly behind current events.

Established biometrics technologies include palm print recognition, fingerprint recognition, hand geometry, dynamic signature, vascular pattern recognition, iris recognition, face recognition, and speaker recognition. Emerging biometrics technologies include rapid DNA forensics, tattoo recognition, stand-off iris recognition, all-aspect face recognition, facial aging, behavioral biometrics, and social and demographic signatures.

Technologies for biographic identity resolution include name matching and name transliteration. We believe more technical progress can be made in these areas, along with the broader problem of probabilistic identity resolution from multiple sources of evidence.

Choosing authentication strategies to match the practical and policy constraints of a given government or private-sector use case will become more complex in coming years. Developing strategies for authentication and other Identity Management actions in the face of compromised databases is an emerging challenge that cannot be ignored. Beyond that, authentication strategies also need to be weighed against various classic vectors, such as effectiveness, sustainability, adaptability in the face of new and evolving threat, as well as against some of the "softer" vectors such as public acceptability and ease of use. More work needs to be conducted to find the correct balance for a given need. A representative sample of what such a balance would look like is in Figure 25.

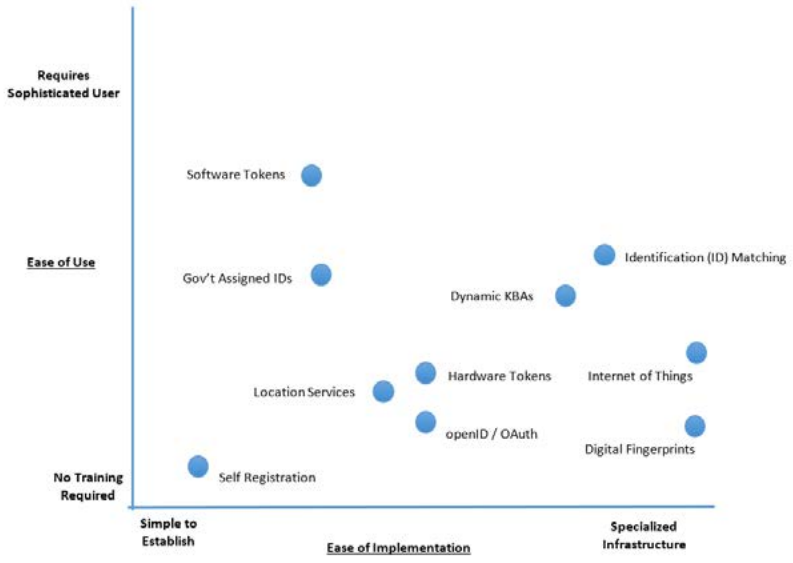

Figure 25. Authentication Strategies Mapped Against Ease of Use and Ease of Implementation

Global Landscape

Many countries have adopted ISO standards relating to fingerprints and other biometrics information and practices, typically based on strong ANSI input. Nations leading in biometrics innovation and investment include the United States, France, Italy, Germany, China, Japan, and South Korea. The community underwent considerable consolidation in the mid-2000s due to venture capital investments, with long-standing technology providers combining to form a handful of larger companies that exist today.

The biometrics device business is heavily globalized. For example, some key U.S. technical commercial assets are currently operating as part of the French firm Sagem, with appropriate safeguards. Around the world, national citizen identification shows a real diversity of approach, with different jurisdictions using identification numbers and a variety of paper or electronic credentials for a range of purposes, including control of internal migration.

The EURODAC (European Dactyloscopy) fingerprint repository for asylum-seekers and irregular border crossers provides an interesting example of biometric identification in service of a special international need. Identity management in networked computer systems and cyberspace is heavily influenced by U.S.-based multinational corporations, such as Microsoft and Oracle. However, governance over the Internet and the activities it supports is being contested internationally, and the national security institutions of each nation respond to the challenge of identity, both in the real and virtual worlds, in their own ways, in keeping with their perceived national interests. (A comprehensive review of those activities is outside the scope of this document.)

Some sources project that by 2020, global mobile biometric market revenues will reach $34.6B annually (see Figure 26). This includes 4.8 billion biometrically enabled smart mobile

devices generating $6.2B in biometric sensor revenue, 5.4 billion biometric app downloads generating $21.7B in annual revenues from direct purchase and software development fees, and 807 billion biometrically secured payment and non-payment transactions generating $6.7B in authentication fees [61].

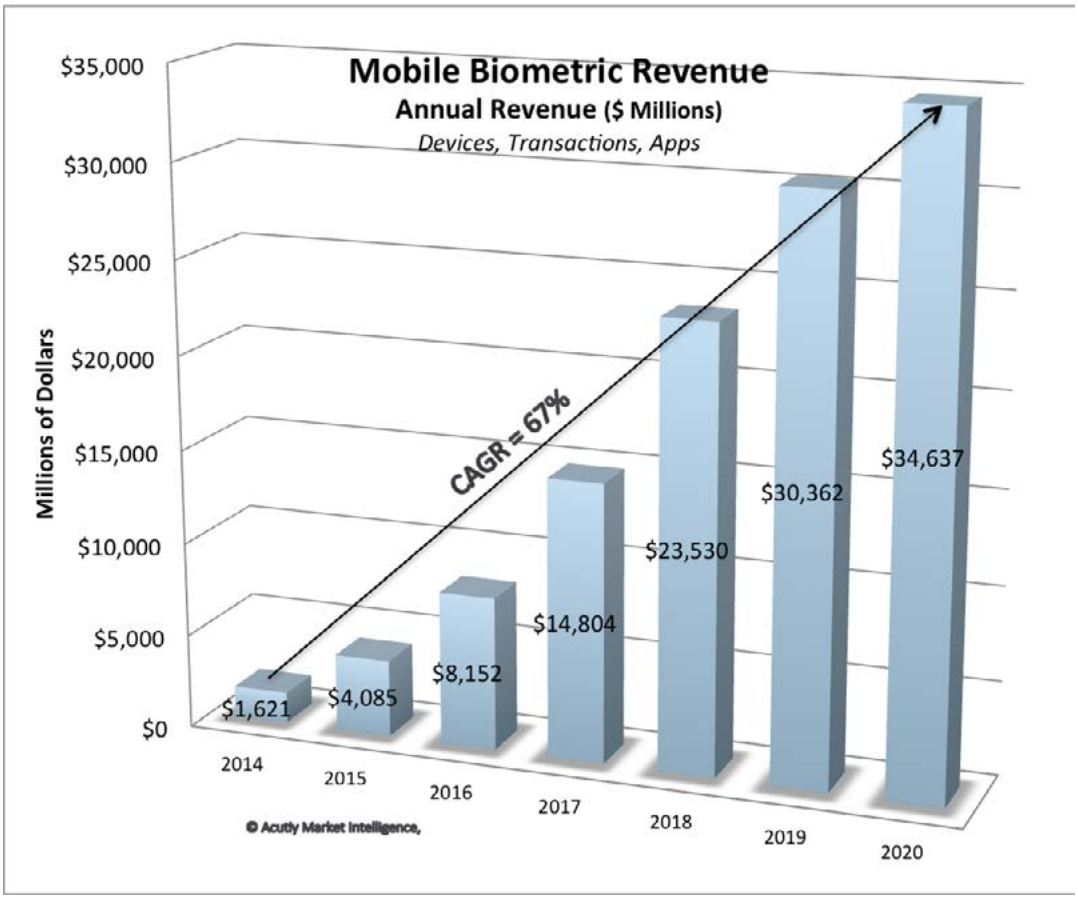

Figure 26. Global Projections of Mobile Biometrics Revenue

In terms of global threat actors, cybercriminal organizations in Eastern Europe, Russia, China, and elsewhere have had notorious successes against numerous corporate and individual targets, stealing large identity datasets for subsequent criminal use. More troubling is the compromise of federal personnel records on an unprecedented scale, which has been attributed to Chinese hackers. The possibilities afforded an adversary with possession of such a massive and relevant dataset speak for themselves, and illustrate the need for maintenance of personal knowledge in identity verification.

Russian state capabilities in cyber warfare have been demonstrated publically on several occasions, and identity compromise is certainly within their scope. The mesh of criminal and state actors in some nations raises additional concerns. Non-state actors have resorted to cyber techniques for some years (e.g., the so-called "electronic jihad" of the previous decade), and must be added to the list of potential threats to online identities. Figure 27 charts the largest data breaches across the globe over the past few years.

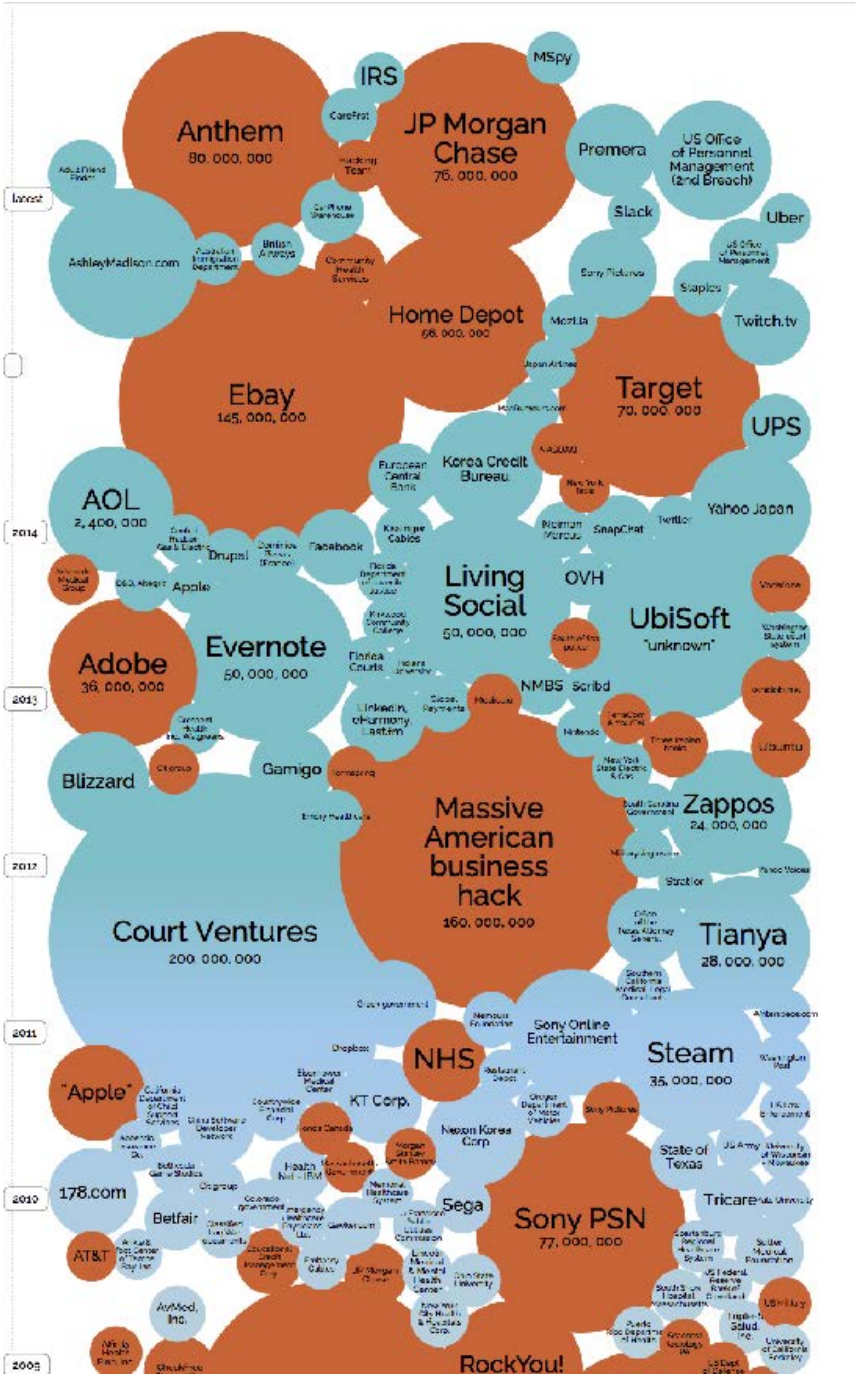

Figure 27. World's Biggest Data Breaches [45]

Within the various Internet and Social Media communities that are used globally by a variety of people, from students to merchants to NGOs to violent extremists, the degree to which identity can be reliably determined varies a great deal by context. Conversely, various foreign governments and other actors do sometimes attempt to compromise these online identities in the furtherance of their own goals.

National Landscape

A subsidiary of the National Security Council established the Biometric Consortium in 1992 as a government-only collaboration forum. Over time, it evolved into a public-private collaboration venue chaired by the National Security Agency and NIST. The consortium holds an annual conference to facilitate scientific and technical interchanges between the U.S. government and outside entities on biometric and other identity technologies in support of defense, homeland security, identity management, border crossing, and electronic commerce. The consortium collaborates with the Armed Forces Communications and Electronics Association (AFCEA) to host the annual Global Identity Summit (GIS), which is the U.S. government's primary outreach and collaboration-building event (and the world's largest identity-focused event. It is designed to 1) promote a high-level understanding of current capabilities, pending needs, and future directions of both the federal government and the identity community, and 2) initiate and advance public-private and cross-discipline collaboration necessary for the continued advancement and appropriate application of identity capabilities.

Until recently, the advancement of biometrics and identity management capabilities has been driven to meet national and homeland security concerns. Policy initiatives spanning three presidential administrations provide a strategic framework for biometrics and identity management in the United States, including:

- Homeland Security Presidential Directive (HSPD)-6 (September 16, 2003), "Integration and Use of Screening Information," and Homeland Security Presidential Directive/HSPD-11 (August 27, 2004), "Comprehensive Terrorist-Related Screening Procedures" provided a policy framework for the comprehensive collection, integration, and use of biometric and biographic information in the counter-terrorism context.
- Homeland Security Presidential Directive/HSPD-12 (August 27, 2004), "Policy for a Common Identification Standard for Federal Employees and Contractors" established a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).
- National Security Presidential Directive (NSPD)-59/Homeland Security Presidential Directive (HSPD) – 24 (June 5, 2008), "Biometrics for Identification and Screening to Enhance National Security," established a framework to ensure federal departments and agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of known and suspected terrorists and others with national security concerns in a lawful and appropriate manner, while respecting privacy and other legal rights under U.S. law.

The National Science and Technology Council Subcommittee on Biometrics and Identity Management played a major role in guiding whole-of-government biometrics and identity management advancement, implementation, and integration over a dozen years following the 9/11 terrorist attacks. Its charter expired in 2012.

The National Strategy for Trusted Identities in Cyberspace (NSTIC), signed by President Obama in 2011, recognized the weaknesses in existing online identity management approaches and laid out guidance to strengthen this key infrastructure through the establishment of an Identity Ecosystem. This ecosystem is a collection of interoperable identity management protocols and implementations that provide strong authentication while requiring minimal personal disclosure during transactions. NIST manages the NSTIC National Program Office, which collaborates with the private-sector Identity Ecosystem Steering Group to meet the goals of NSTIC.

Identity capabilities have been transitioning away from federal security initiatives over the past 12 to 18 months, as the community's predominant focus shifts to private-sector initiatives involving technologies used for security and user-convenience applications. Inclusion of identity capabilities in recent smartphone versions has led to a more knowledgeable and experienced population, which is driving expectations for similar capabilities within other domains.

Key government actors include the DHS Office of Biometric Identity Management, the DoD Biometrics and Defense Forensics and Biometrics Agency, the FBI Biometrics Center of Excellence, the NIST Biometrics Resource Center, and certain Intelligence Community programs. NIST plays a very useful role in stimulating biometrics research through a series of competitive technology evaluations such as the TATT-C tattoo recognition evaluation in 2015. NIST evaluations and grand challenges have played a leading role in the strategic advancement of a number of identity technologies.

Industry Landscape

Key U.S. biometrics systems vendors include MorphoTrak, MorphoTrust, Cogent, NEC, and a number of smaller players. The emphasis in this field has moved from single-modality systems (e.g., fingerprints) to multi-modal systems (e.g. fingerprints and iris and facial recognition). In the realm of biographic identity matching systems, systems vendors in the national security space include BASIS Technologies, IBM, and SRA. Note that IBM has consolidated the technologies of a variety of smaller vendors. Other vendors, such as ArgoData, serve the healthcare market segment, and Internet companies (such as Google, Face Book, Microsoft, Apple, Twitter, Skype) are advancing technologies in the realm of Internet Identity Management.

Primary industry-collaboration bodies include the International Biometrics and Identification Association (predominantly focused on technology providers) and the Fast Identity Online (FIDO) Alliance (primarily focused on supporting online users of identity).

Figure 28 details Acuity's Mobile Biometric Market Landscape (MBML). This model provides some insight into how the mobile biometric market might evolve. Though every application and use case may not fit neatly within its constraints, the model provides a useful tool for evaluating how the market will develop, where organizations fit, and what type of competition will be encountered. Not surprisingly, authentication volume and assurance levels have an inverse relationship. Assurance requirements increase as they move from day-to-day

consumer use, to more secure enterprise applications, to the highest level of secure government solutions for military and intelligence operations. Conversely, authentication volumes grow from millions to billions to trillions as solutions move from externally vetted and authenticated high-security environments with centrally stored biometrics templates, to self-authentication on personal devices for locally managed consumer applications [62].

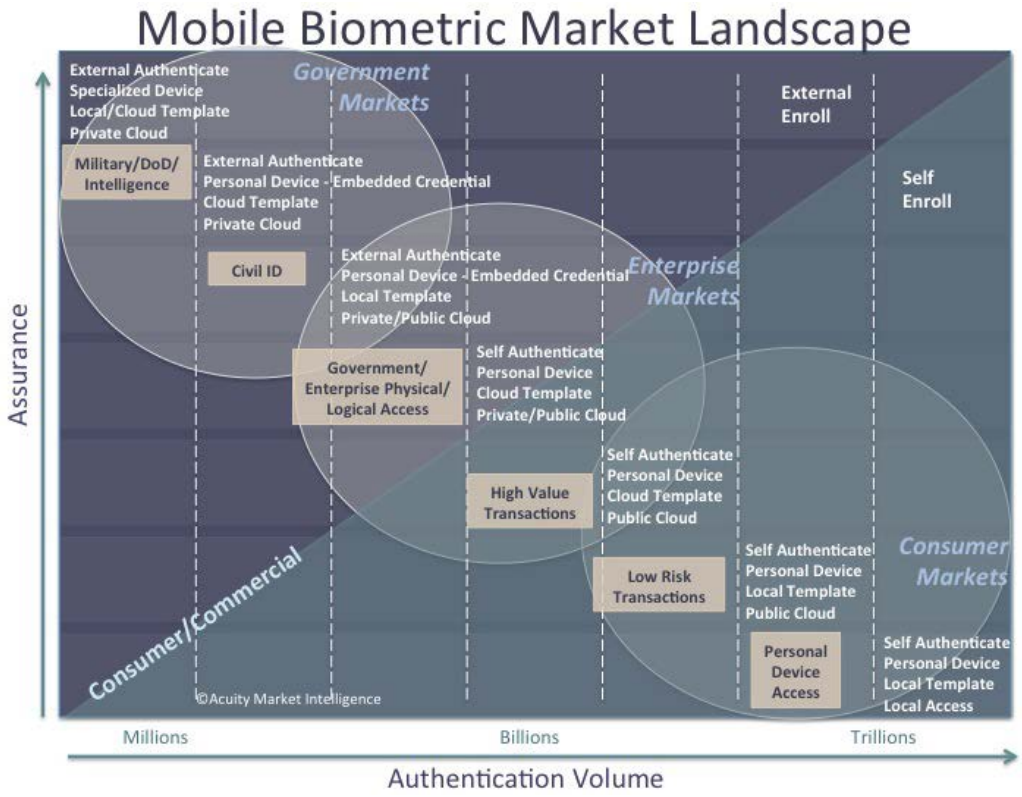

Figure 28. Acuity's Mobile Biometric Market National Landscape

Looking Forward

The preponderance of digital identities and mobile devices, and law enforcement's limited capacity to respond to identity fraud and the loss or misuse of identity information, suggests ongoing vigilance is required. The following measures are worthy of consideration over the next 4 to 10 years:

- Examine and reinvigorate interagency cooperation in biometrics and identity management at all echelons of government.
- Assess legal and governance processes lagging behind technical capabilities; regularly review information sharing between inter-agency uses requiring efficiencies as well as safeguards.
- Continue and expand the use of NIST competitive evaluations to advance the state of the art in biometric technologies, forensics, and virtual identity.

- Critically examine and make research and engineering investments in biometrics system interoperability, especially on a cross-agency basis.
- Critically examine and make research and engineering investments in open, non-proprietary evaluation methodologies for all identity systems.
- Address through research, engineering, and policy the key problem of Identity Management Under Attack: the erosion of knowledge-based authentication when the attacker has as much information as the defender due to compromised data stores (Identity Management war games, and multi-factor identifiers may be useful here).
- Make research and engineering investments in emerging biometric technologies and biographic modalities, including rapid DNA forensics, tattoo recognition, hyper-spectral and stand-off iris, all-aspect face recognition, behavioral biometrics, facial aging, vulnerabilities, social and demographic signatures, and probabilistic identity resolution from multiple sources of evidence.

Internet of Things

Introduction

The Internet of Things (IoT) refers to a decentralized inter-connected network of devices (e.g., sensors and actuators), applications, and services that are deployed on a massive scale for sensing, controlling, and interacting with the physical world. Gartner defines the IoT as *a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.*

What all definitions agree on is the fact that IoT does not represent a single technology. Nor does it constitute a system that is carefully designed, deployed, and managed like other networks and systems. Rather, IoT is a *disruptive change* that is already upon us, albeit in its early stages, and is evolving rapidly in ways that are not completely predictable.

We know that IoT enables operational capabilities and experiences far surpassing anything we have known to date from computer systems. It also presents unprecedented opportunities in the private and public sectors, from efficient management of our physical infrastructure to real-time response to natural or man-made disasters. At the same time, it presents serious vulnerabilities and operational risks that need to be understood and managed to the extent possible.

Gartner projects that by the end of 2015, 4.9 billion connected things will be in use, which is a 30 percent increase from 2014. By 2020, it will reach 25 billion things [63]. The IoT is becoming a driver for business transformation and its disruptive effect will be sensed across all industries and sectors of society.

Its rise is predicted to bring major disruption to many market sectors. Impacts could include:

- **Healthcare:** Remote patient monitoring using smart devices, allowing patients and their doctors to obtain real-time access to health data, resulting in the potential for reduction of healthcare costs, improved quality of care, and better health outcomes.

- **Transportation:** Development of intelligent transportation infrastructure from roads to airports to parking garages, along with connected and self-driving vehicles.
- **Energy:** Smart-grid technologies with the ability to drive efficiencies in energy production and consumption.
- **Manufacturing:** Potential dramatic process improvements would include improved automation, increased ability for proactive maintenance, and better decision making.
- **Government:** Impact in the public sector will range from defense and emergency services to service delivery and responsiveness to citizen needs.

Figure 29 presents an enterprise view of IoT in which some of these domains are called out, along with related technologies. Initial projections indicate that the IoT will be the largest device market, out pacing that of the smartphone, personal computer, tablet, connected car, and the wearable market combined.

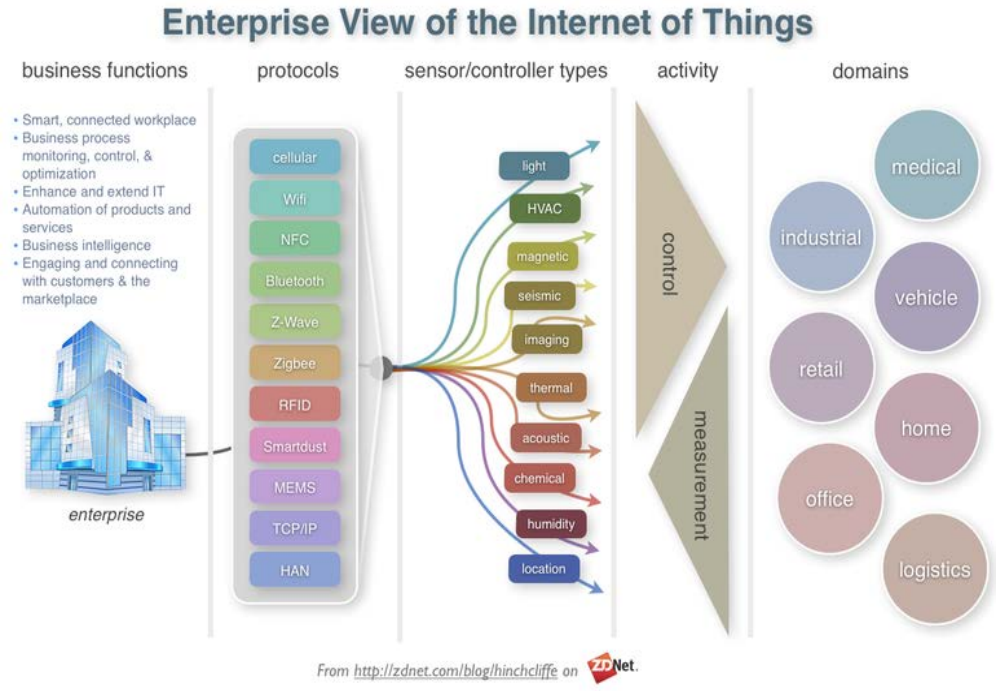

Figure 29. IoT Enterprise View of Impacted Domains, Enabling Protocols, and Sensor/Actuator Types [64]

Landscapes

The current IoT landscape can be characterized, in part, by considering the number of connected devices in use today. Some estimates put the current number at close to 15 billion globally. This is expected to increase dramatically, with some estimates as high as 200 billion—30 billion of those being "autonomous things"—by the end of 2020 [65]. Whether or not these estimates prove to be accurate, there is no denying that the number of networked sensors, actuators, and smart devices will continue to increase in the near to mid-term.

The applications for the IoT chains of devices range from smart homes and cities to healthcare. Unfortunately, there is limited data available on each application area. Figure 30 is an attempt to rank order the top 10 IoT application areas, based on social media data collected from Twitter, Google and LinkedIn.

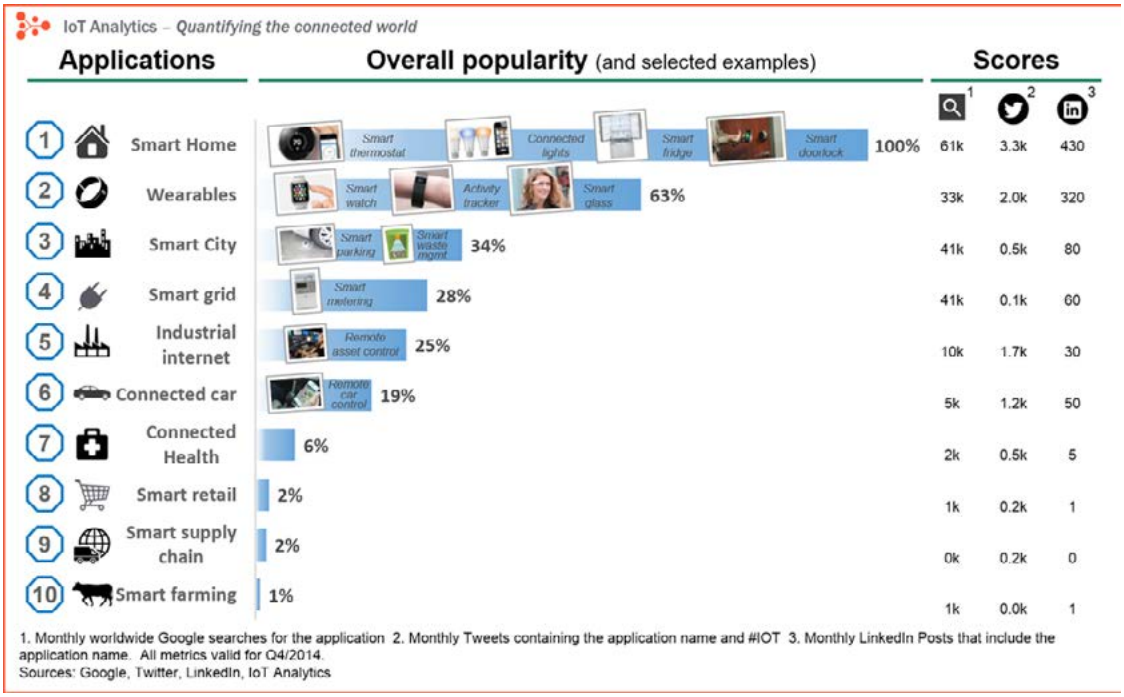

Figure 30. Relative Ranking of IoT Applications Based on Social Media Data Mining [66]

The connectedness promised by IoT presents great potential opportunities for the public and private sectors. However, it also poses significant threats and vulnerabilities for consumers, manufacturers, and government organizations alike. Chief among these concerns is security.

According to a recent SANS study on securing the IoT (see Figure 31), respondents were asked to indicate the greatest threat to IoT systems over the past five years. The results, depicted in Figure 32, show device patching topping the list at 31 percent.

Vulnerability scanning and patching is made particularly challenging by the lack of discovery and identification capabilities available for today's IoT devices and systems. In recognition of this issue, MITRE will host an international "Challenge" in 2016 in search of innovative solutions for device discovery and identification. In addition to improving the security posture for IoT, such a discovery and identification capability will be fundamental to improving operations and management, as well as for optimizing performance and situational awareness.

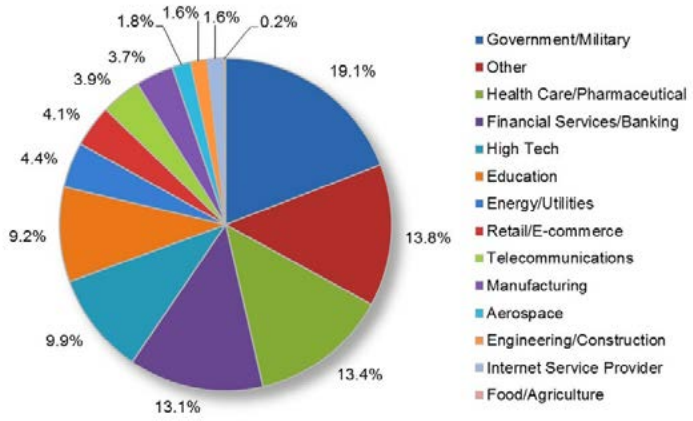

Figure 31. Respondent Industry Representation for SANS Survey

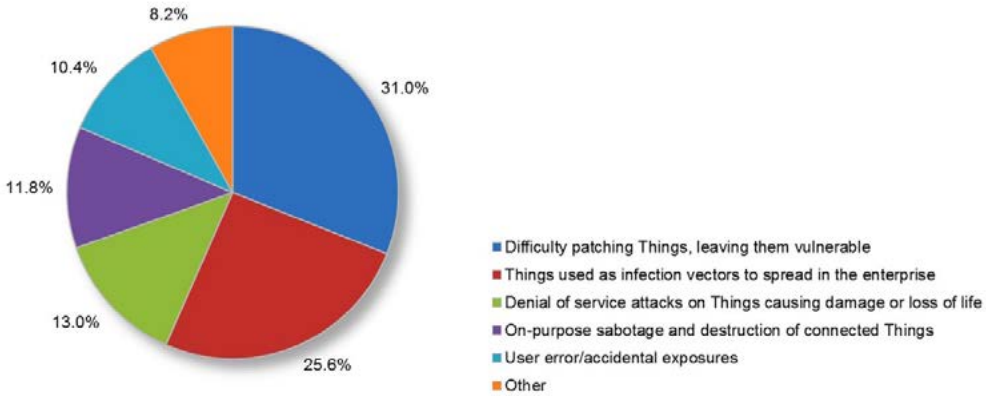

Figure 32. Perceived Security Threats to IoT

A security vulnerability not specifically called out in the SANS survey, but critically important to U.S. government and military interests, is *supply chain integrity*. Supply chain counterfeits and compromised components could ultimately account for a substantial portion of the IoT landscape. Threats include independent and state-sponsored actors secretly inserting malicious code into both hardware and software during the manufacture of internet enabled "things." Detecting and mitigating the risk of supply chain counterfeits and compromised components requires the analysis of both processes and the technical implementation of hardware/software elements.

There is ongoing private and public R&D activity around many of these security topics, as well as large-scale design and integration challenges. Many universities, for example, have developed capabilities that are directly related to either large-scale IoT research or one of the enabling technologies for IoT. The following list, while not intended to be exhaustive, describes some of the top institutions conducting IoT research:

- Georgia Tech: Center for the Development and Application of Internet of Things Technologies
- Massachusetts Institute of Technology (MIT): Media Lab

- University of California (UC) Berkley: Interactive Device Design, Critical Making, Wireless Sensor Networks
- UC Irvine: Laboratory for Ubiquitous Computing and Interaction
- UC Los Angeles: Networked & Embedded Systems Laboratory
- Cornell University: Interaction Design Lab
- Carnegie Mellon: Connected Embedded Systems
- University of Washington: Ubiquitous Computing Lab
- New York University: Interactive Telecommunications Program
- Georgia Institute of Technology: Ubiquitous Computing Group
- Ryerson University, Canada: Ubiquitous and Pervasive Computing Lab
- University of Wisconsin–Madison: Internet of Things Lab
- Purdue: M2M Labs

In the corporate world, Apple and Google top the list of most influential IoT companies. Both have made substantial investments, which underline the fact that IoT is now a strategic imperative for the world's largest technology companies. Figure 33 lists the top 10 most influential IoT companies according to a 2014 Appinions survey, with the caveat that Google's 2014 purchase of Nest is not represented. Intel, Microsoft and Cisco follow close behind.

Figure 34 illustrates the results of an IoT analytics data collection study, based on social media sources, which rank orders the top 20 companies. This graphic presents data for Quarter 1 (Q1) 2015 and provides comparisons to Q4 2014. These results are consistent with those in Figure 33, with the exception of IBM, which does not appear in the Appinions study.

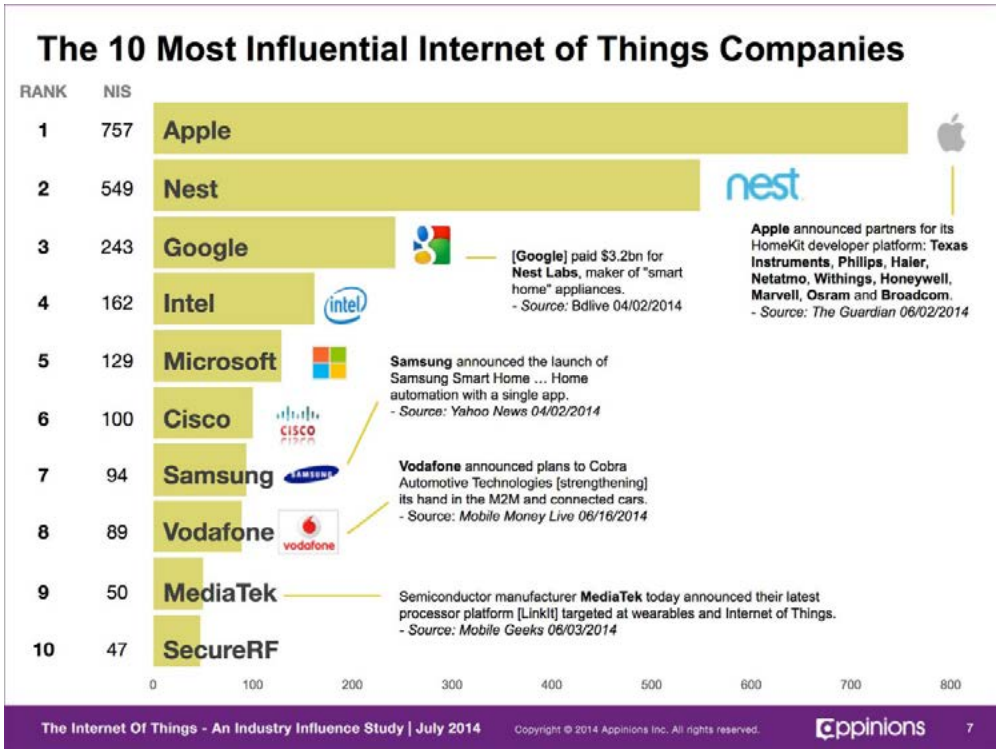

Figure 33. List of Top 10 IoT Companies According to 2014 Appinions Study

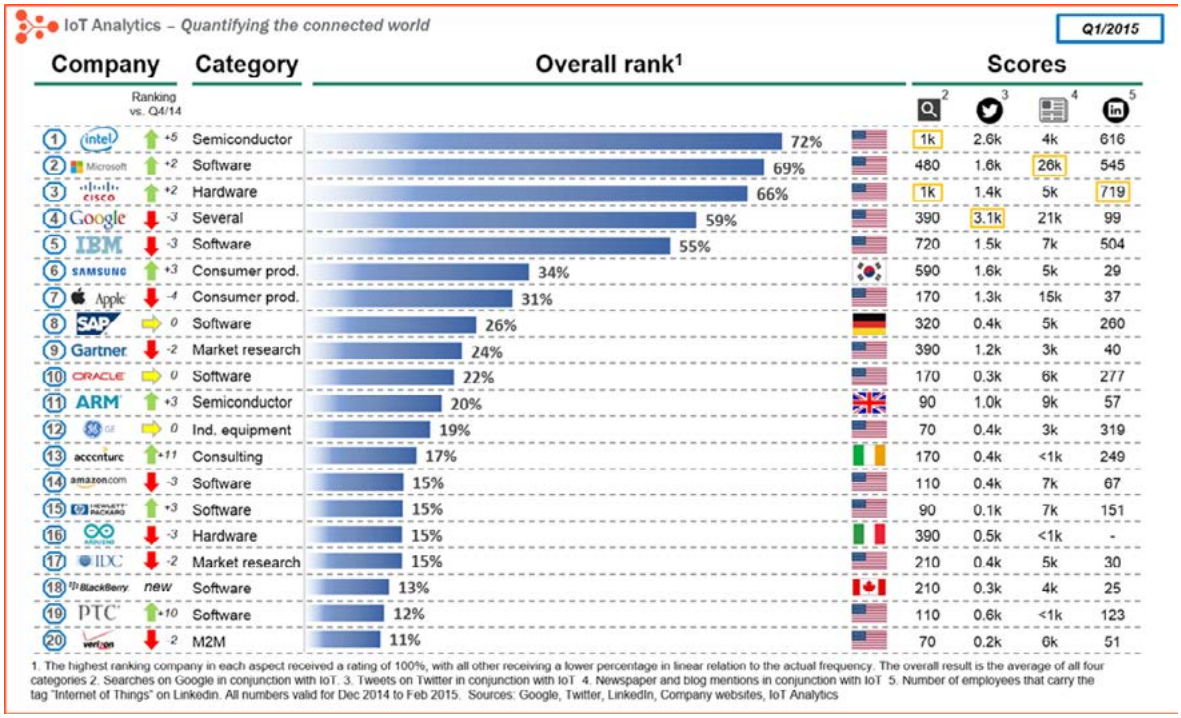

Figure 34. Top 20 IoT Companies According to IoT Analytics
Data Gleaned from Social Media Sources

Looking Forward

The Internet of Things will proliferate rapidly over the next few years as networked devices, including sensors, actuators, and a host of smart devices, continue to come online. The IoT will not only have a huge impact on the consumer market, these devices will increasingly be embedded into the nation's critical infrastructure and military systems. This makes it especially important to understand the implications of this particular technological evolution on our social and political fabric, both positive and negative.

The U.S. government will not be the major driving force behind the IoT wave, which is already building faster and higher than most government organizations had expected. Rather, we believe that there is a window of opportunity within which the government can properly study and understand the radical changes and implications that will be wrought by such a massive scale of connectedness across the globe. With a more well-informed approach to IoT, the government will be positioned to benefit from, and properly use, the vast array of capabilities that will emerge. Perhaps more importantly, however, the government will be in a stronger position to mitigate the risks manifest in IoT.

The government has already started to begin formulating a clearer picture of IoT and what it means for the future. The Federal Trade Commission (FTC) recently released a staff report that summarizes much of what was learned at a 2013 workshop titled *The Internet of Things: Privacy and Security in a Connected World* [67]. While the report did a good job of illuminating serious security and privacy concerns, it also highlighted the need for a more mature, and deep, understanding of IoT. Such an understanding may require concerted efforts by the government to commission and support studies that bring together the national labs, industry partners, academia, FFRDCs, and other government leaders.

The U.S. government is already accepting IoT into applications that touch federal entities. IoT affects each federal department in different ways and agencies need to coordinate and integrate their efforts to successfully incorporate IoT components in a secure and interoperable manner. There is opportunity to apply innovation to improving intuitive and secure user interfaces, securing communications protocols, and mitigating risk while minimizing impact on user experience.

In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) released a report on IoT that laid out many of the challenges and opportunities [68]. The NSTAC report illuminates the need for a more serious commitment to study, and ultimately mitigate, the impacts that IoT is capable of having on critical infrastructure and other important areas.

There are also other areas of concern to address, which were not included in the FTC and NSTAC reports. One is the very real potential that such a rapidly evolving complex system as IoT could produce "emergent behavior" that is every bit as disruptive as intentionally malicious activity. Classical approaches to design, engineering, and security do not translate well to systems of the size and scope of IoT. At the federal level, devices that interoperate across

organizations have the potential to aggregate sensed information to higher national security classifications or unintended disclosure of personally identifiable information.

Other areas include the implications of not having the ability to execute centralized control, counter-measures to mitigate supply-chain incidents, and dealing with the possibility of IoT ultimately becoming a ubiquitous *sensing and actuation utility* [69] on which adversaries and allies alike can develop and deliver applications and services.

These and many other challenges underscore the need for a proactive and well-formulated federal strategy for studying and shaping the future state of IoT. While the government may not be driving the IoT revolution, it has the opportunity to influence its adoption and reduce risks to the nation and its critical infrastructure. Applying resources to this problem now, and bringing together the best of academia, national labs, and FFRDCs to address them, will position the nation more favorably to handle what lies ahead.

Trustworthy Autonomy

Introduction

The DoD defines an autonomous system as one that is able to "make decisions and react without human interaction" [70]. In the near future, we are likely to see increasingly autonomous systems helping to diagnose illnesses and determine courses of treatment, make investment decisions for individuals, and analyze large volumes of intelligence data to make conclusions about security risks. Further in the future, we are likely to see autonomous delivery vehicles (in the air and on the ground), driverless taxi-cabs, container ships that unload themselves, aircraft that refuse to crash, mines operated by just a handful of individuals, and combat aircraft that can penetrate air defenses without a pilot onboard.

Today's automation system researchers, designers, and developers are building complex, interconnected, non-deterministic, adaptive systems to improve people's safety, security, and prosperity. Our common vernacular often refers to such systems as "autonomous." Algorithms used in "autonomous" systems tend to be so sophisticated they are not simply measuring the environment with sensor data but *perceiving* what the measurements may mean (often referred to as perception). Decision algorithms go beyond simple heuristics (e.g., if-then) to algorithms that reason and make judgments about the correct course of action.

The difference between an automated system and an autonomous system lies in the decisions being made. A system that decides to turn on the furnace in a home because the temperature falls below a set level is an automated system (better known as a thermostat). A system that figures out that the furnace needs to be turned on because people in the room are putting on sweaters, shivering, and making verbal comments about being cold is an autonomous system because it uses *perception* of a variety of complex indicators to *reason* that there is a need for increased temperature, and thus the furnace should be turned on.

For the purposes of this section, we will be discussing information technology with algorithms that perceive the environment and use reasoning techniques to make judgments regarding the appropriate course of action and are able to act without direct human oversight. We will follow the lead of a recent National Research Council study and use the term "increasingly autonomous systems" [71] to refer to complex automation systems that are becoming more sophisticated, interconnected, non-deterministic, and adaptive.

As an example, consider facial recognition software, which was first developed for security and law enforcement purposes and can now be found on our home computers and on social networking sites. Just a few decades ago, the effectiveness of such algorithms was limited, producing significant misdetections and false matches. Today, not only has the effectiveness increased, but the performance of such algorithms has increased to the point that they are available for use on mobile devices.

While facial recognition software might not seem to fit into a discussion of autonomous systems, the algorithms associated with the perception and recognition of facial features are very sophisticated. Thirty years ago, we may have described a computer system that could recognize a person in a video or photograph as being part of an artificial intelligence system. The amazing has become routine [72].

As automation technology has increased in sophistication, it has become more connected, adding to its complexity. For example, within the Internet of Things (IoT), we are connecting household appliances—and even ourselves—to an information network. At the same time, we are increasing the amount of data we collect about everyday life and automating more and more of life's everyday processes.

These complex interconnected automation systems (often referred to as a "system-of-systems" [73])[4] with potentially limitless sources of data input boggle the imagination. More and more of the algorithms running on these systems are becoming non-deterministic in that they can exhibit different behaviors on different runs (even for seemingly the same input). Non-deterministic algorithms are often used by developers when an approximate solution may suffice because they tend to be efficient (either during development or run-time execution) when compared to deterministic algorithms.

To ensure that these systems are able to respond to a changing environment and assist in development of algorithms where it is impractical to develop an explicit algorithm using heuristics, developers employ a variety of machine learning capabilities. Sometimes a system is adaptive during its life cycle, theoretically improving its performance with additional data and experience. This means that the system may behave differently over time as it experiences different environmental conditions. Machine learning often relies on pattern recognition and other computational statistical techniques. As an example, the abilities of facial recognition software improve over time as more and more confirmed matches are made.

4. A system-of-systems is "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities."

Some of the potential characteristics of these increasingly autonomous systems, which may or may not be present in each specific system, are listed below.

Characteristic	Present
Reacts at cyber speed	Usually
Reduces tedious tasks	Usually
Augments human decision makers	Usually
Proxy for human actions or decisions	Usually
Robust to incomplete or missing data	Usually
Reacts to the environment	Usually
Exhibits emergent behavior	Usually
Adapts behavior to feedback (learns)	Usually
Responds differently to identical inputs	Usually
Addresses situations beyond the routine	Usually
Reduces cognitive workload for humans	Usually
Replaces human decision makers	Potentially
Robust to unanticipated situations	Usually
Behavior determined by experience rather than by design	Usually
Adapts behavior to unforeseen environmental changes	Potentially
Makes value judgments (weighted decisions)	Usually
Makes mistakes in perception and judgment [71]	Potentially

These increasingly autonomous systems are not necessarily intended to work independently from human decision makers and, in many applications, are part of a human–machine team. The machine–human interaction adds yet another layer of complexity to the use and regulation of autonomous systems.

Increasing autonomy—whether part of a cyber–physical system (e.g., unmanned vehicles, the power grid, medical devices, command and control systems) or part of a purely cyber system (e.g., high frequency trading, medical diagnosis, intelligence analysis)—presents many challenges for the government, which acts as an acquirer, provider, and regulator of these technologies. These issues will be discussed in the Looking Forward section.

Landscapes

In a recent survey of aerospace, defense, and security experts, 70 percent of them identified the development of autonomous vehicles and related technologies as being a key area of development in the next three years [20]. The U.S. DoD and other federal agencies have identified autonomous systems as a key game changer [74], [71], [75], [76]. It is difficult to fully quantify the implications of increasingly autonomous systems and the level of R&D investment worldwide due to the somewhat imprecise nature of what is considered an autonomous system vs. a sophisticated piece of information technology. The two areas often overlap.

Today, industry is investing many orders of magnitude more money than the government in advanced automation system capabilities. Investors include multibillion information technology companies, such as Google, Amazon, Microsoft, Apple, Cisco, IBM, and General Electric; well–capitalized new entrants, such as Tesla Motors; and start–ups, such as Cruise Automotive.

National Landscape

California's Silicon Valley is a hot bed of activity in autonomous systems for both established giants and new entrants. Many innovations are coming from companies started by professors or graduates associated with Carnegie Mellon University, Massachusetts Institute of Technology, and Stanford University. Interestingly, much of the autonomous system research at these academic institutions received some level of government funding.

Much of the information about industry's research activities is proprietary and thus limited—until a company is getting ready to market its technology. Some of the advances shared by industry include:

- Apple is building a self-driving car in Silicon Valley and scouting secure locations in the San Francisco Bay area to test it [77].
- Tesla Motors is testing its latest Autopilot feature (version 7.0) with a select number of Model S beta testers; this technology includes a highway auto-steer capability (essentially lane keeping) and automatic parallel parking, as well as improved Traffic-Aware Cruise Control [78]. Tesla CEO Elon Musk claims that his cars will be fully autonomous in five or six years [79].
- Delphi Automotive demonstrated its full suite of Advanced Drive Assistance Systems by driving cross country from San Francisco to New York City with 99 percent of the highway driving conducted in autonomous driving mode [80].
- Using a machine learning approach called cognitive computing, IBM continues to improve Watson, a generalized inference engine that is being used for a variety of knowledge work applications—from call-center problem solving to oncology diagnosis [81]. (The Department of Veterans Affairs is exploring use of IBM's Watson for clinical diagnosis.)
- Another pioneering company is planning to design, build, and sail the world's first full-sized, fully autonomous unmanned vessel across the Atlantic Ocean. The Mayflower Autonomous Research Ship will use state-of-the-art wind and solar technology for its propulsion, enabling an unlimited range [82].
- John Deere is selling the Tango E5, an "autonomous lawnmower" that automatically navigates around a lawn area that is defined by a boundary wire. Loaded with a number of different sensors to ensure safe operation, it cuts the grass and recharges itself as needed [83].

Global Landscape

While the United States has been the international leader in innovation associated with automation and information technology for many years, other countries are now catching up. For example, Germany, Australia, the United Kingdom, Japan, Israel, China, and India are not only demonstrating technology innovation in the area, they are also quickly putting the technology into operational mode.

Examples of this include:

- The largest number of unmanned aircraft sold worldwide is produced by China's Da-Jiang Innovations (DJI) Science and Technology Co., Ltd. The company manufactures a variety of unmanned aircraft models for the recreational market as well as commercial market (65 percent of the applications for Federal Aviation Administration exceptions are being granted to operators intending to fly a DJI product) [84].
- The Port of Brisbane in Queensland, Australia, is one of the most automated container ports in the world with 30 automated straddle carriers [85].[5]
- Also in Australia, Rio Tinto, with its Mine of the Future™ program, is the largest owner and operator of autonomous trucks in the world and has a fleet moving tons of material in Pilbara, Western Australia [86].
- Three German carmakers (Audi, BMW, and Daimler) have teamed to acquire Nokia's digital mapping business in a bid to outsmart information technology groups in the race to cash in on the driverless car revolution [87].
- The Iron Dome anti-rocket system, used by the Israeli Defense Forces as a defense against rocket attacks from the Gaza Strip, can detect and intercept incoming rockets and projectiles using automatic mechanisms. The system is developed in Israel by Rafael Advanced Defense Systems and Israel Aircraft Industries [88].

Looking Forward

Government and industry continues to work on the many challenges surrounding increasingly autonomous systems. This includes the technical challenges of creating algorithms associated with the perception and reasoning capabilities required for operations. In the past, such technology revolutions would not be possible without significant government R&D investment to ensure innovation. As with the IT revolution, however, the potential for significant ROI means private industry is investing in the R&D that will lead to many, if not most, of the significant innovations expected in the autonomous system area.

Government, however, has a critical role to play in the future of autonomous systems as the objective regulator that will ensure the safety and security of the American public. We all see the benefits of this revolution, as systems becoming increasingly intelligent, moving toward a state in which the "machine" perceives, learns, decides, and acts—often without human engagement. However, government agencies must ensure that these sophisticated, non-deterministic software systems can be trusted to do what they are designed to do and remain resilient to design defects, unanticipated situations or data, and deliberate attack. While industry is involved in addressing the methods, metrics, and enablers associated with determining the competency of autonomous systems to function as intended, this is not their first priority. Neither can they look across the industry as can the government.

To this end, the United States needs to advance its mechanisms and policies for oversight, testing and evaluation, and certification of autonomous systems. It is especially important to

5. Asciano is the operator of the automated Fisherman's Island portion of the Port of Brisbane.

ensure the resiliency of systems which, if they fail or underperform, could trigger dire consequences from a safety, security, or prosperity perspective.

To address these concerns, the DoD has formed an S&T-oriented Community of Interest (COI) focused on autonomy. The Autonomy COI has four working groups with one specifically focused on Test and Evaluation/Validation and Verification (TEVV) of autonomy. The TEVV Working Group has released a Technology Investment Strategy that identifies challenges and research gaps in this area, laying out five specific goals for strategic technology investment [89]. Similarly, in 2014 the National Research Council (NRC) released a study on autonomy requested by NASA that identified barriers to adoption of autonomy and laid out a research agenda in eight specific areas [71]. While the NRC study focused on civil aviation, much of the research agenda can be generalized to a broad spectrum of applications.

The DoD COI on Autonomy conducted a survey of research efforts associated with DoD autonomous systems. Of the $149M spent yearly on autonomy research, only about $9M (or approximately 6 percent) was devoted to research associated with TEVV (mostly research into methods to evaluate the dependability of autonomous technologies). See Figure 35.

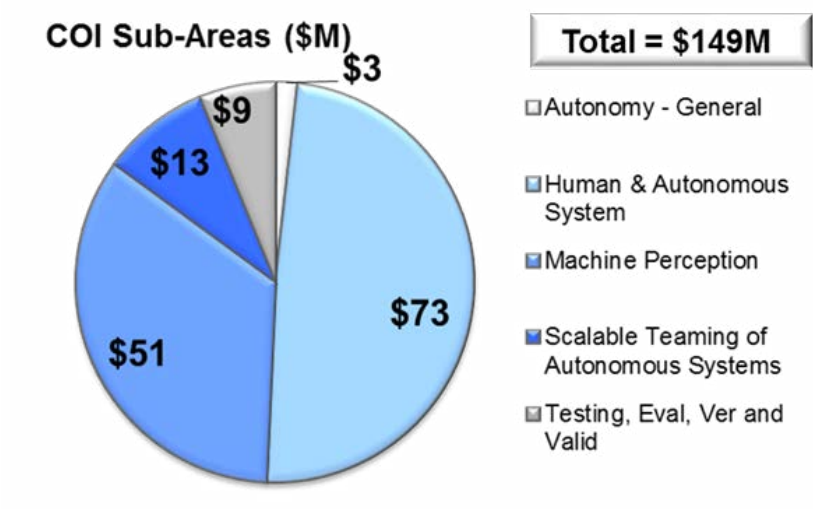

Figure 35. U.S. Department of Defense Investment in Autonomy by Area of Focus [90]

It seems that the area of establishing methods, metrics, and techniques for calibrating the trustworthiness of increasingly autonomous systems is being under-addressed. (It is possible, of course, that efforts associated with establishing the enablers associated with trustworthy autonomy may be hiding under the labels of other research efforts, such as: Trusted Computing, Cybersecurity, Software Reliability and Resiliency, Software Assurance, Liability Attribution, Complexity Research, Software Forensics, Airworthiness–Safety Cases, Trusted E-Commerce, and/or Software TEVV.)

Policy

The government must also examine the policy implications of autonomous systems. For example, as these systems gain the authority for more and more complex decisions, there will be significant issues with regard to the liability and responsibility for those decisions. The DoD has already developed a specific policy with regard to the role of autonomous or semi-autonomous capabilities in weapon systems [91]. While much of the authority to engage specific targets will remain with the human operator, the kill-chain is becoming increasingly reliant on a variety of complex automation systems that analyze intelligence information that is used to "find and fix" potential targets.

Government regulators will also need to establish new oversight policies associated with automated driving capabilities in automobiles. Currently, the National Highway Traffic Safety Administration regulates required safety equipment and monitors the performance of consumer automobiles; for example, it issues recalls as appropriate. However, it does not currently have a role in determining if the automation systems offered for commercial sale in automobiles will function at an acceptable level of safety risk (including vulnerabilities to deliberate attacks).

The individual states regulate and license human drivers today. But who will license an automation system that is functioning as a human driver? Some states have established policies for the testing of automated driving capabilities but no state has established regulations for operating a "self-driving" automobile. Some people believe today's tort and product liability laws are sufficient to address these possibilities—while some people believe the government needs to take another look at these laws [92].

Many technical innovators in industry worry that liability and other policy concerns will be a larger barrier than technology in the realization of increasingly autonomous systems. The government needs to understand the technology and the future scenarios to enable new autonomous technology while at the same time protecting the public.

References

[1] Executive Office of the President, "A Strategy for American Innovation," The White House, Washington, D.C., 2011.

[2] D. Steinbock, "American Innovation Under Structural Erosion and Global Pressures," The Information Technology & Innovation Foundation, Washington, D.C., 2015.

[3] Organisation for Economic Co-Operation and Development, "OECD.Stat – Patents by technology," Stat technology | © OECD, [Online]. Available: http://stats.oecd.org/Index.aspx?DatasetCode=PATS_IPC. [Accessed 8 April 2016].

[4] The Hay Group and Partnership for Public Service, "Leading Innovation in Government," 2011. [Online]. Available: http://www.haygroup.com/downloads/us/leading_innovation_in_government_-_a_study_with_the_partnership_for_public_service_and_hay_group.pdf. [Accessed 8 April 2016].

[5] J. Tidd and J. Bessant, "Innovation Portal Toolkit: Technology Forecasting," John Wiley and Son Ltd, April 2016. [Online]. Available: http://www.innovation-portal.info/toolkits/technological-forecasting/. [Accessed 8 April 2016].

[6] The National Institute of Standards and Technology (NIST), "NIST General Information," The National Institute of Standards and Technology (NIST), 8 January 2016. [Online]. Available: http://www.nist.gov/public_affairs/general_information.cfm. [Accessed 8 April 2016].

[7] PricewaterhouseCoopers, "Innovation: Government's Many Roles in Fostering Innovation," January 2010. [Online]. Available: http://www.pwc.com/gx/en/technology/pdf/how-governments-foster-innovation-2010.pdf. [Accessed 8 April 2016].

[8] U.S. General Services Administration, "Challenge.gov About," [Online]. Available: https://www.challenge.gov/about/. [Accessed 8 April 2016].

[9] T. Kalil and N. Maynard, "US Ignite: A New Foundation for America's Broadband Future (Blog)," The White House, 12 September 2011. [Online]. Available: https://www.whitehouse.gov/blog/2011/09/12/us-ignite-new-foundation-america-s-broadband-future. [Accessed 8 April 2016].

[10] The White House, "Startup America," 31 January 2011. [Online]. Available: https://www.whitehouse.gov/economy/business/startup-america. [Accessed 8 April 2016].

[11] National Science Foundation, "National Robotics Initiative (NRI)," Directorate for Computer & Information Science & Engineering, [Online]. Available: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503641&org=CISE. [Accessed 8 April 2016].

[12] The White House, "Fact Sheet: U.S. Global Development Policy," Office of the Press Secretary, 22 September 2010. [Online]. Available: https://www.whitehouse.gov/the-press-office/2010/09/22/fact-sheet-us-global-development-policy. [Accessed 8 April 2016].

[13] P. Singer, "Federally Supported Innovations: 22 Examples of Major Technology Advances that Stem from Federal Research Support," February 2014. [Online]. Available: http://www2.itif.org/2014-federally-supported-innovations.pdf. [Accessed 8 April 2016].

[14] V. Bush, "Science The Endless Frontier," July 1945. [Online]. Available: http://www.nsf.gov/about/history/nsf50/vbush1945.jsp. [Accessed 8 April 2016].

[15] R. Spinard, F. Orr, E. Stofan, L. Tabak and C. Woteki, "Chief Scientists: U.S. Can Remain Innovation Leader in Science's 'Endless Frontier'," The Huffington Post, 6 August 2015. [Online]. Available: http://www.huffingtonpost.com/dr-richard-w-spinrad/chief-scientists-us-can-r_b_7948522.html?utm_hp_ref=science&ir=Science. [Accessed 8 April 2016].

[16] National Science and Technology Council, "Science for the 21st Century," July 2004. [Online]. Available: https://www.whitehouse.gov/files/documents/ostp/NSTC%20Reports/Science-21Century.pdf. [Accessed 8 April 2016].

[17] The White House, "National Science and Technology Council," [Online]. Available: https://www.whitehouse.gov/administration/eop/ostp/nstc. [Accessed 10 April 2016].

[18] President's Council on Advisors on Science and Technology, "Transformation and Opportunity: The Future of the U.S. Research Enterprise," November 2012. [Online]. Available: https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_future_research_enterprise_20121130.pdf. [Accessed 10 April 2016].

[19] The White House, "Office of Science and Technology Policy About PCAST," 19 December 2011. [Online]. Available: https://www.whitehouse.gov/administration/eop/ostp/pcast/about. [Accessed 10 April 2016].

[20] Battelle and R&D Magazine, "2014 Global R&D Funding Forecast," December 2013. [Online]. Available: http://www.battelle.org/docs/tpp/2014_global_rd_funding_forecast.pdf. [Accessed 10 April 2016].

[21] The White House, "OMB Circular A-11, Section 84—Character Classification (Schedule C)," 2015. [Online]. Available: https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s84.pdf. [Accessed 10 April 2016].

[22] National Science Foundation, "Business Research and Development and Innovation Survey (BRDIS)," 4 June 2013. [Online]. Available: http://www.nsf.gov/statistics/srvyindustry/#tabs-1. [Accessed 10 April 2016].

[23] Thomson Reuters, "2015 National Capital Venture Association Yearbook," March 2015. [Online]. Available: http://nvca.org/?ddownload=1868. [Accessed 10 April 2016].

[24] Committee on Research Universities; Board on Higher Education and Workforce; Policy and Global Affairs; National Research Council, "Research Universities and the Future of America: Ten Breakthrough Actions Vital to Our Nation's Prosperity and Security," The National Academies Press, 2012. [Online]. Available: http://www.nap.edu/catalog/13396/research-universities-and-the-future-of-america-ten-breakthrough-actions. [Accessed 10 April 2016].

[25] ShanghaiRanking Consultancy, "Academic Ranking of World Universities 2014," 2014. [Online]. Available: http://www.shanghairanking.com/ARWU2014.html. [Accessed 10 April 2016].

[26] Executive Office of the President: President's Council of Advisors on Science and Technology, "Report to the President – Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Mathematics," February 2012. [Online]. Available: https://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-executive-report-final_2-13-12.pdf. [Accessed 2016 April 2016].

[27] D. DeSilver, "Growth from Asia drives surge in U.S. foreign students," Pew Research Center, 18 June 2015. [Online]. Available: http://www.pewresearch.org/fact-tank/2015/06/18/growth-from-asia-drives-surge-in-u-s-foreign-students/. [Accessed 17 April 2016].

[28] L. Chang, "International Student Mobility Trends 2014: The Upward Momentum of STEM Fields," World Education News & Reviews, 3 March 2014. [Online]. Available: http://wenr.wes.org/2014/03/international-student-mobility-trends-2014-the-upward-momentum-of-stem-fields/. [Accessed 17 April 2016].

[29] U.S. Citizenship and Immigration Services, "Extending Period of Optional Practical Training by 17 Months for F-1 Nonimmigrant Students With STEM Degrees and Expanding Cap-Gap Relief for All F-1 Students With Pending H-1B Petitions," Department of Homeland Security, 8 April 2008. [Online]. Available: http://www.uscis.gov/iframe/ilink/docView/FR/HTML/FR/0-0-0-1/0-0-0-145991/0-0-0-163040/0-0-0-164807.html. [Accessed 17 April 2016].

[30] National Math + Science Initiative, "STEM Education Statistics," 2016. [Online]. Available: https://www.nms.org/AboutNMSI/TheSTEMCrisis/STEMEducationStatistics.aspx. [Accessed 17 April 2016].

[31] Gartner, Inc., "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor," 18 August 2015. [Online]. Available: http://www.gartner.com/newsroom/id/3114217. [Accessed 17 April 2016].

[32] United States Government Printing Office, "United States Code 42 USC § 5195c. Critical infrastructures protection," [Online]. Available: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf. [Accessed 17 April 2016].

[33] Department of Homeland Security, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," February 2010. [Online]. Available: http://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf. [Accessed 17 April 2016].

[34] National Infrastructure Advisory Council, "Critical Infrastructure Resilience Final Report and Recommendations," 8 September 2009. [Online]. Available: http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf. [Accessed 18 April 2016].

[35] The White House Office of the Press Secretary, "Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience," The White House, 12 February 2013. [Online]. Available: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Accessed 18 April 2016].

[36] Department of Homeland Security, "The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets," February 2003. [Online]. Available: http://www.dhs.gov/national-strategy-physical-protection-critical-infrastructure-and-key-assets. [Accessed 18 April 2016].

[37] The White House Office of the Press Secretary, "Executive Order -- Improving Critical Infrastructure Cybersecurity," The White House, 12 February 2013. [Online]. Available: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. [Accessed 18 April 2016].

[38] Lloyd's and the University of Cambridge Judge Business School, Centre for Risk Studies, "Emerging Risk Report – 2015, Business Blackout: The insurance implications of a cyber attack on the US power grid," May 2015. [Online]. Available: https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf. [Accessed 18 April 2016].

[39] Department of Homeland Security, Homeland Security Council, "National Strategy For Homeland Security," October 2007. [Online]. Available: http://www.dhs.gov/national-strategy-homeland-security-october-2007. [Accessed 18 April 2016].

[40] Department of Homeland Security, "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience," 2013. [Online]. Available: http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. [Accessed 18 April 2016].

[41] Electric Power Research Institute (EPRI), "Our Business," Electric Power Research Institute, Inc., 2016. [Online]. Available: http://www.epri.com/About-Us/Pages/Our-Business.aspx. [Accessed 18 April 2016].

[42] University of Illinois at Urbana-Champaign, "Critical Infrastructure Resilience Institute," Center of Excellence by the Department of Homeland Security Science and Technology Directorate , 2016. [Online]. Available: http://ciri.illinois.edu/. [Accessed 18 April 2016].

[43] Critical Utility Infrastructural Resilience (CRUTIAL), "Publications," Nukedit, [Online]. Available: http://crutial.rse-web.it/Dissemination/PUBLICATIONS.asp. [Accessed 18 April 2016].

[44] National Infrastrucure Advisory Council, "National Infrastructure Advisory Council Critical Infrastructure Security and Resilience National Research and Development Plan: Final Report and Recommendations," Department of Homeland Security, 14 November 2014. [Online]. Available: http://www.dhs.gov/publication/niac-cisr-national-rd-plan-final-report. [Accessed 18 April 2016].

[45] Information is Beautiful, "World's Biggest Data Breaches," Information is Beautiful, 16 February 2016. [Online]. Available: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. [Accessed 18 April 2016].

[46] Executive Office of the President, National Science and Technology Council, "Trustworthy Cyperspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," The White House, December 2011. [Online]. Available: https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf. [Accessed 18 April 2016].

[47] Internet Security Alliance, "The Advanced Persistent Threat: Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing," 6 June 2013. [Online]. Available: http://isalliance.org/publications/2013-06-06-ISA_APT_Paper-Practical_Controls_for_SMBs.pdf. [Accessed 18 April 2016].

[48] E. M. Hutchins, M. J. Clopperty and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, March 2011. [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. [Accessed 18 April 2016].

[49] Bodeau, Graubart, Heinbockel and Laderman, "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques," The MITRE Corporation, McLean, VA, 2015.

[50] Y. Leitersdorf and O. Schreiber, "Cybersecurity Hindsight And A Look Ahead At 2015," Tech Crunch, 28 December 2014. [Online]. Available: http://techcrunch.com/2014/12/28/cyber-security-hindsight-2020-and-a-look-ahead-at-2015. [Accessed 18 April 2016].

[51] Market Research Media, "U.S. Federal Cybersecurity Market Forecast 2017-2022," 23 February 2016. [Online]. Available: http://www.marketresearchmedia.com/?p=206. [Accessed 18 April 2016].

[52] The Networking and Information Technology Research and Development Program, "Supplement to the President's Budget, FY 2014.," May 2013. [Online]. Available: https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=48. [Accessed 19 April 2016].

[53] C. Strohm and T. Shields, "Obama Boosts Pentagon Cyber Budget Amid Rising Attacks," Bloomberg Technology, 11 April 2013. [Online]. Available: http://www.bloomberg.com/news/articles/2013-04-10/lockheed-to-general-dynamics-target-shift-to-cyber-spend. [Accessed 19 April 2016].

[54] Gartner, Inc., "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware," Gartner, 22 August 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2828722. [Accessed 19 April 2016].

[55] Gartner, Inc., "Gartner Magic Quadrant Reports for Cybersecurity-related Categories, 2013-14," [Online].

[56] Tata Consultancy Services, "Companies are spending a lot on big data," Tata Consultancy Services , 1 August 2015. [Online]. Available: http://sites.tcs.com/big-data-study/spending-on-big-data/.

[57] S. Hupfer, "Global Data Analytic Investment," IBM Center for Applied Insight, 2014.

[58] Forbes, "Roundup of Analytic Dig Data Business Intelligence Forecasts and Market Estimates 2014," Forbes, June 24, 2014.

[59] J. Kelly, "Big Data Vendor Revenue and Market Forecast 2012–2017," Wikibon, 19 January 2016. [Online]. Available: http://wikibon.org/wiki/v/Big_Data_Vendor_Revenue_and_Market_Forecast_2012-2017. [Accessed 19 April 2016].

[60] Type Safe, "Cloud Infrastructure Technologies in Use," Type Safe, August 2015. [Online]. Available: http://www.typesafe.com/.

[61] Acuity Market Intelligence, "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy," Acuity Market Intelligence, [Online]. Available: http://www.acuity-mi.com/GBMR_Report.php. [Accessed 19 April 2016].

[62] Acuity Market Intelligence, "Mobile Biometric Market Research, Analysis & Forecasts," Acuity Market Intelligence, [Online]. Available: http://www.acuity-mi.com/Mobile_Biometrics.php. [Accessed 19 April 2016].

[63] Gartner, Inc., "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015," Gartner, 11 November 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2905717. [Accessed 19 April 2016].

[64] D. Hinchcliffe, "Is the Internet of Things strategic to the enterprise?," ZDNet, 31 May 2014. [Online]. Available: http://www.zdnet.com/article/is-the-internet-of-things-strategic-to-the-enterprise/. [Accessed 19 April 2016].

[65] Business Wire, "The Internet of Things Is Poised to Change Everything, Says IDC," Business Wire, 3 October 2013. [Online]. Available: http://www.businesswire.com/news/home/20131003005687/en/Internet-Poised-Change-IDC#.VeCBkU2FN9A. [Accessed 19 April 2016].

[66] IOT Analytics, "IOT Analytics Homepage," IOT Analytics, [Online]. Available: http://iot-analytics.com/. [Accessed 19 April 2016].

[67] Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World, FTC Staff Report," January 2015. [Online]. Available: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. [Accessed 19 April 2016].

[68] The President's National Security Telecommunications Advisory Committee (NSTAC), "NSTAC Report to the President on the Internet of Things," 19 November 2014. [Online]. Available: http://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. [Accessed 19 April 2016].

[69] J. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal,* vol. 1, no. 1, March 2014.

[70] U.S. Department of Defense, "Unmanned Systems Integrated Roadmap FY2013-2038," 2013. [Online]. Available: http://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf. [Accessed 19 April 2016].

[71] Committee on Autonomy Research for Civil Aviation; Aeronautics and Space Engineering Board; Division on Engineering and Physical Sciences; National Research Council, "Autonomy Research for Civil Aviation: Toward a New Era of Flight," The National Academies Press, June 2014. [Online]. Available: http://www.nap.edu/catalog/18815/autonomy-research-for-civil-aviation-toward-a-new-era-of. [Accessed 19 April 2016].

[72] Y. Yang, Y. Li, C. Fermuller and Y. Aloimonos, "Robot Learning Manipulation Action Plans by "Watching" Unconstrained Videos from the World Wide Web," 2015. [Online]. Available: http://

www.umiacs.umd.edu/~yzyang/paper/YouCookMani_CameraReady.pdf. [Accessed 19 April 2016].

[73] U.S. Department of Defense, "Defense Acquisition Guidebook," 16 September 2013. [Online]. Available: https://acc.dau.mil/docs/dag_pdf/dag_complete.pdf. [Accessed 19 April 2016].

[74] Office of the US Air Force Chief Scientist, "Technology Horizons: A Vision for Air Force Science and Technology During 2010–2030," September 2011. [Online]. Available: http://www.defenseinnovationmarketplace.mil/resources/AF_TechnologyHorizons2010-2030.pdf. [Accessed 20 April 2016].

[75] US Army Training and Doctrine Command (TRADOC), "Technology and Capability Objectives for Force 2025 and Beyond," US Army Training and Doctrine Command (TRADOC), Fort Eustis, 2014.

[76] US Navy Office of Naval Research, "Naval S&T Strategic Plan," 1 September 2011. [Online]. Available: http://www.onr.navy.mil/About-ONR/science-technology-strategic-plan/~/media/Files/About-ONR/Naval-Strategic-Plan.ashx. [Accessed 20 April 2016].

[77] The Guardian, "Documents confirm Apple is building self-driving car," The Guardian, 2016. [Online]. Available: http://www.theguardian.com/technology/2015/aug/14/apple-self-driving-car-project-titan-sooner-than-expected. [Accessed 20 April 2016].

[78] A. Hard, "Autopilot goes beta: Tesla running semiautonomous trials with Model S owners," Digital Trends, 19 August 2015. [Online]. Available: http://www.digitaltrends.com/cars/tesla-self-driving-autopilot-begins-beta-testing-pictures/. [Accessed 20 April 2016].

[79] A. Hard, "Tesla CEO: Our cars will be fully autonomous 'in the five or six-year time frame'," Digital Trends, 15 September 2014. [Online]. Available: http://www.digitaltrends.com/cars/tesla-ceo-cars-will-fully-autonomous-five-six-year-time-frame/. [Accessed 20 April 2016].

[80] Delphi Automotive LLP, "Delphi Drive," Delphi Automotive LLP, [Online]. Available: http://www.delphi.com/delphi-drive. [Accessed 20 April 2016].

[81] IBM, "Meet Watson – The platform for cognitive business," IBM Watson, [Online]. Available: http://www.ibm.com/smarterplanet/us/en/ibmwatson/index.html. [Accessed 20 April 2016].

[82] Scuttlebutt Sailing News, "Coming Attraction: Ocean Crossing Autonomous Trimaran," Scuttlebutt Sailing News, 18 August 2015. [Online]. Available: http://www.sailingscuttlebutt.com/2015/08/18/coming-attraction-ocean-crossing-autonomous-trimaran/. [Accessed 20 April 2016].

[83] John Deere, "Tango E5," John Deere, 2016. [Online]. Available: https://www.deere.com/en_INT/products/equipment/autonomous_mower/tango_e5/tango_e5.page#viewTabs. [Accessed 20 April 2016].

[84] The MITRE Corporation, "MITRE analysis of publicly available Section 333 filing data available on FAA's web-site," The MITRE Corporation, McLean.

[85] Asciano, "Asciano Australia Homepage," Asciano, 24 February 2016. [Online]. Available: https://asciano.com.au. [Accessed 20 April 2016].

[86] Rio Tinto, "Rio Tinto improves productivity through the world's largest fleet of owned and operated autonomous trucks," Rio Tinto, 9 June 2014. [Online]. Available: http://www.riotinto.com/media/media-releases-237_10603.aspx#.dpuf. [Accessed 20 April 2016].

[87] The Guardian, "Vorsprung durch technik: US tech giants v Germany in the driverless car race," The Guardian, 2016. [Online]. Available: http://www.theguardian.com/business/2015/aug/04/vorsprung-durch-technic-us-tech-germany-driverless-car. [Accessed 20 April 2016].

[88] The Jerusalem Post, "Is Israel's Iron Dome the precursor to futuristic 'killer robots'?," The Jerusalem Post, 2016. [Online]. Available: http://www.jpost.com/Israel-News/Is-Israels-Iron-Dome-the-precursor-to-futuristic-killer-robots-396680. [Accessed 20 April 2016].

[89] Office of the Assistant Secretary of Defense For Research & Engineering, "Department of Defense Research & Engineering Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group Technology Investment Strategy 2015 - 2018," US Department of Defense, May 2015. [Online]. Available: http://www.defenseinnovationmarketplace.mil/resources/OSD_ATEVV_STRAT_DIST_A_SIGNED.pdf. [Accessed 20 April 2016].

[90] Community of Interest, "Communities of Interest Investment Data," Community of Interest, 2014. Also: www.defenseinnovationmarketplace.mil/resources/AutonomyCOI_NDIA_Briefing20150319.pdf.

[91] Department of Defense, "Directive Number 3000.09: Autonomy in Weapon Systems," 21 November 2012. [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf. [Accessed 20 April 2016].

[92] J. Villasenor, "Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation," The Brookings Institution, 24 April 2014. [Online]. Available: http://www.brookings.edu/research/papers/2014/04/products-liability-driverless-cars-villasenor. [Accessed 20 April 2016].

List of Acronyms

A

AAAS	American Association for the Advancement of Science
AFIT	Air Force Institute of Technology
ANL	Argonne National Laboratory
ANSI	American National Standards Institute
APT	adv anced persistent threat
ARRA	American Recovery & Reinvestment Act
ASU	Arizona State University

B

B	billion
BI	business intelligence
BNL	Brookhaven National Laboratory

C

CAC	Common Access Card
CAGR	Compound Annual Growth Rate
CAMS	Computing and Analytical Methods Subcommittee
CEO	Chief Executive Officer
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIRI	Critical Infrastructure Resilience Institute
CISR	Critical Infrastructure Security and Resilience
COE	Center of Excellence
COI	Community of Interest
COTS	commercial off-the-shelf
CPS	cyber-physical systems
CRUTIAL	Critical Utility Infrastructural Resilience
CSC	Computer Sciences Corporation

D

DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DJI	Da-Jiang Innovations
DNA	deoxyribonucleic acid
DoD	Department of Defense
DOE	Department of Energy

E

EERA	European Energy Research Alliance
EIFER	European Institute for Energy Research
EO	Executive Order
EPRI	Electric Power Research Institute
E.U.	European Union

F

FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FTC	Federal Trade Commission
FY	Fiscal Year

G

GCC	Government Coordinating Council
GDP	Gross Domestic Product
GIS	Global Identity Summit
GOTS	government off-the-shelf

GPS	Global Positioning System

H

HHS	U.S. Department of Health and Human Services
HILF	high-impact, low-frequency
HP	Hewlett-Packard
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

I

IC	Intelligence Community
ICS	industrial control systems
ID	identification
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Lab
IoT	Internet of Things
IP	intellectual property
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology

J, K

KBA	Knowledge Based Authentication

L

LANL	Los Alamos National Lab

M

M&S	Modeling & Simulation
M	million
MBML	Mobile Biometric Market Landscape
ML	machine learning

N

NAS	National Academies of Science
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Center of Excellence
NERC	North American Electric Reliability Corporation
NGO	Non-Governmental Agency
NIAC	National Infrastructure Advisory Council
NIH	National Institutes of Health
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NRC	National Research Council
NSF	National Science Foundation
NSPD	National Security Presidential Directive
NSTAC	National Security Telecommunications Advisory Committee
NSTB	National SCADA Test Bed
NSTC	National Science and Technology Council
NSTIC	National Strategy for Trusted Identities in Cyberspace

O

ORNL	Oak Ridge National Laboratory
OT	Operational Technology

P

PCAST	President's Council of Advisors on Science and Technology
PIN	personal identification number
PNNL	Pacific Northwest National Laboratory

PPD	Presidential Policy Directive

Q

Q	Quarter

R

R&D	Research and Development
RMM	Resilience Management Model
ROI	Return on Investments

S

S&T	Science & Technology
SAIC	Science Applications International Corporation
SCADA	Supervisory control and data acquisition
SCC	Sector Coordinating Council
SEI	Software Engineering Institute
SFI	Santa Fe Institute
SNL	Sandia National Lab
SoS	system–of–systems
SSA	Sector–Specific Agency
STEM	Science, Technology, Engineering, and Math
STIX	Structured Threat Information eXpression

T

T	trillion
TAXII	Trusted Automated Exchange of Indicator Information
TEVV	Test and Evaluation/Validation and Verification
TransCARE	Transmission Contingency and Reliability Evaluation
TTPs	tactics, techniques, and procedures

U, V

UC	University of California
U.K.	United Kingdom
UN	United Nations
U.S.	United States
USDA	United States Department of Agriculture
UVA	University of Virginia

W, X, Y, Z

WTC	World Trade Center