NEW AMERICA

CYBERSECURITY INITIATIVE

ROBERT J. BUTLER AND IRVING LACHOW

SMART CITY PARTNERSHIPS

Smart Cities and the Internet of Things: Benefits, Risks, and Options

OCTOBER 2016

About the Authors

Robert J. Butler is the co-founder and managing director of Cyber Strategies LLC. Previously, he served as the Chief Security Officer for IO, a global data center service and product firm. Earlier in his career, Butler served as the first Deputy Assistant Secretary of Defense for Cyber Policy. He is a retired U.S. Air Force colonel and a former member of the Defense Department's Senior Executive Service. Butler earned a bachelor of science degree in computer information systems from Manhattan College and a master of business administration from the School of Business at the University of Maryland.

Irving Lachow joined MITRE in 2010 as a Principal Cyber Engineer. He has worked on and led a number of projects across a range of cyber policy and technology areas for the Department of Defense, the intelligence community, and the Department of State. Lachow is currently a Portfolio Manager and is leading the company's international cyber outreach activities. In addition to working at MITRE, Lachow is a non-resident fellow at the Center for Strategic and International Studies, an affiliate at Stanford University's Center for International Security and Cooperation, and an advisor to the Mach37 Cyber Accelerator.

Dr. Lachow's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

Acknowledgments

The authors would like to especially thank Mrs. Kathryn Butler for her tireless efforts in reviewing and editing this article. Kristi's attention to detail and patience in combing through our many drafts was invaluable and greatly improved the quality of our work. Thank you, Kristi!

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies, and for individuals.

Find out more at **newamerica.org/cybersecurity-initiative**.

Contents

Introduction	2
Challenges of Urbanization	2
The Internet of Things and Smart Cities	4
IoT Threats and Risks	6
Building Partnerships, Building Trust	7
Public-Private Partnership Models	8
Next Steps	9
Notes	11

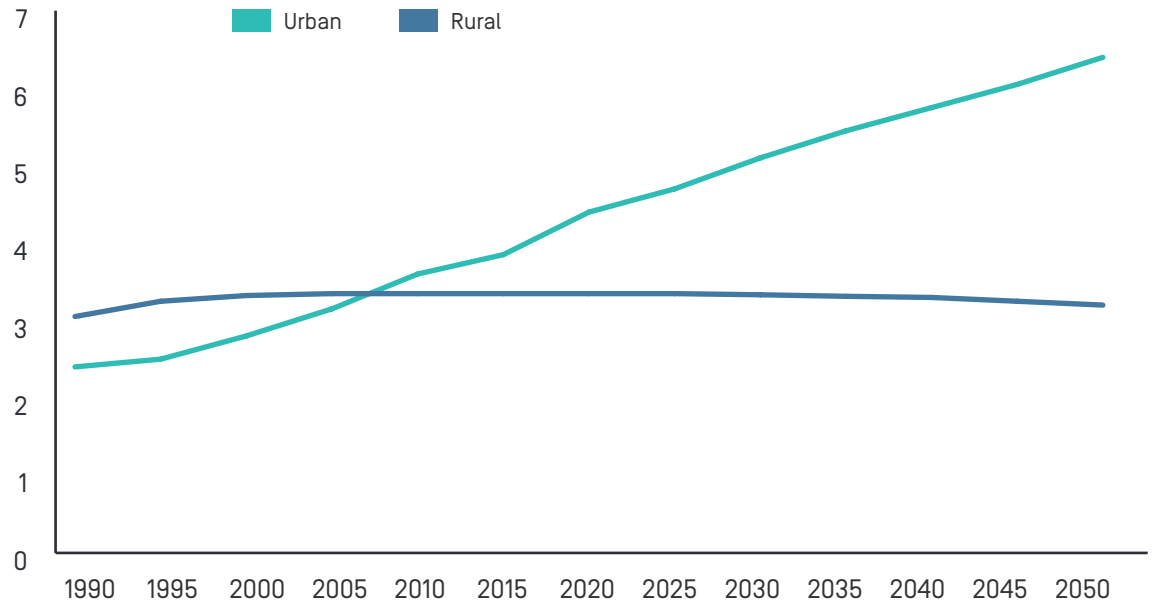
INTRODUCTION

Cities generate over 70 percent of the world's gross domestic product (GDP). Most industries and commercial entities are located in or in the vicinity of urban areas.[1] As urbanization increases, cities—especially in underdeveloped nations—will face a host of challenges. Information and communications technologies (ICT) provide great opportunities for overcoming these challenges and improving overall economic well-being for city dwellers and workers.[2] Efforts to utilize ICT in urban centers are often referred to as "Smart Cities" initiatives. While Smart Cities rely on a host of different ICT, one of the most important technological developments underlying these efforts is the Internet of Things (IoT). IoT promises a wide range of benefits to Smart Cities, but also carries a number of serious cybersecurity risks. This paper examines how IoT might be used to support Smart Cities, explores the cybersecurity risks associated with IoT technologies, and proposes a number of steps that might be taken to address those risks.

CHALLENGES OF URBANIZATION

Over 50 percent of the world's seven billion people live in cities today.[3] That number will grow to 70 percent by 2050.[4] (See Figure 1).[5] Almost half of this anticipated increase is projected to occur in Asia.[6] This paper highlights a few of the challenges associated with this growth—mobility, traffic, energy provisioning, crime, and governance—but others, such as pollution and education, are equally important.

Figure 1 | Urban and Rural World Population (in billions), 1990-2050



Mobility is a key dynamic of urbanization. According to a report on mobility published by the UN Habitat for a Better Urban Future, "by 2005, approximately 7.5 billion trips were made in cities worldwide each day. In 2050, there may be three to four times as many passenger-kilometers travelled as in the year 2000. Freight movement could also rise more than threefold during the same period." [7] As urban population growth continues so does "urban sprawl," resulting in longer commuting distances to work and services. The UN report on mobility further expounds, "this leads to a growing dependency on private motorized transport and other car-centered mobility. Consequently, widespread congestion and traffic gridlock have now become the norm in many cities, impacting urban life through negative externalities such as pollution, noise, stress, and accidents."[8] Traffic will get much worse unless something fundamental changes.

The availability of secure, reliable energy is foundational to urban development. Digital energy (that is, energy used to power ICT) is required for businesses and data centers that drive many municipal services. Looking into the future, the Electric Power Research Institute estimates that data centers alone could reach 20 percent of power consumption in the United States by the year 2030.[9] The current energy infrastructure found in most cities around the world is inadequate to meet these demands. We need innovative solutions to energy generation, transmission, and distribution to meet the needs of current and future city dwellers.

Traffic and power consumption are not the only trends unique to cities. A direct correlation can be made between urbanization, particularly in developing countries, and increasing levels of crime, violence, and lawlessness. The UN Habitat for a Better Future has posited "that 60 percent of urban residents in the developing world have been victims of crime at least once over the past five years. The growing violence and feeling of insecurity that city dwellers are facing daily is one of the major challenges around the world."[10]

At its most basic level, governance is the process by which public policy decisions are made and implemented. It encompasses a constellation

of relationships between a wide range of stakeholders.[11] Governance of a city can include legal frameworks and political, managerial, and administrative processes that enable the local government to respond to the needs of citizens. The explosive population growth in cities complicates governance by increasing the diversity of needs and cultural approaches to problem solving, adding in multiple communities, neighborhoods, and ethnic groups. This added complexity is pushing cities to develop smart and adaptable governance structures, enabled by ICT, that provide tailored services for their citizens.

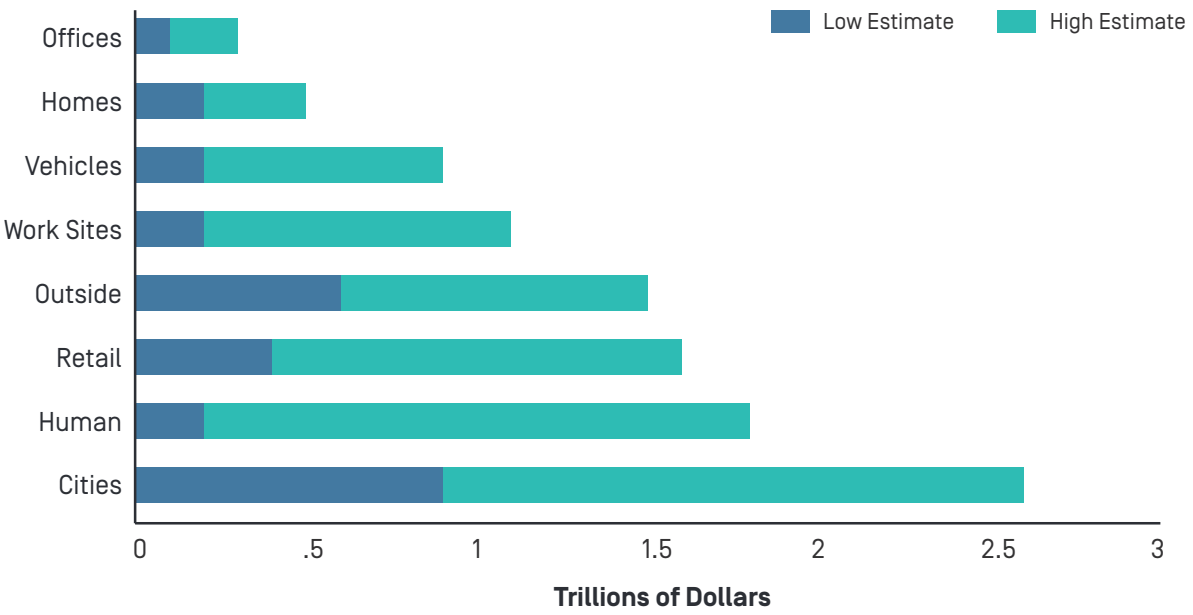
THE INTERNET OF THINGS AND SMART CITIES

The "Internet of Things" describes the ability to connect any Internet Protocol-enabled device to the Internet. According to one Big Data report, "These devices could include your thermostat, your car, or a pill you swallow so the doctor can monitor the health of your digestive tract."[12] The number of new devices and services built for the IoT has significantly risen in recent years, and industry forecasters estimate that 26-50 billion connected devices will be in use worldwide by 2020.[13] With the number devices exponentially increasing each year, the IoT could offer a potential global economic impact of $4 trillion to $11 trillion a year by 2025. (See Figure 2).[14] The greatest impact is likely to be felt in urbanized areas where IoT devices and "smart" technologies have the capability to leverage high-speed communication networks to bolster infrastructure and services such as water and electricity supplies, sanitation and waste management, urban mobility and public transport, IT connectivity, public safety, and weather monitoring.[15]

In 2014, shortly after his government was sworn in, Indian Prime Minister Narendra Modi announced his vision to establish 100 smart cities throughout the country. He defined a smart city as a city equipped with basic infrastructure to give a decent quality of life and a clean and sustainable environment through application of smart solutions. Modi's concept of smart solutions revolves around three areas:

- Electronic dissemination of information between local governments and citizens to automatically "push" advisories and enable rapid citizen feedback
- Improved energy management though the use of automated metering controls and green building development
- Advanced analytics and intelligent traffic management systems to support efficient use of the urban road infrastructure network[16]

Figure 2 | Potential Global Economic Impact, by settings that use IoT



Modi's concept for smart cities and the use of ICT for enabling smart solutions is not confined to India. Many smart cities are using ICT to enable new ways of managing city transportation systems, distributing digital energy, controlling traffic, and monitoring environmental pollution.[17] Within smart cities, building automation technology is providing significant advances in physical security, space cooling and heating, and lighting controls. Developments in manufacturing technology help drive continuous condition monitoring, smart factories, and wireless, mobile supply chain tracking. Smart grids and electric vehicle infrastructure are offering great promise for improved efficiency in energy-constrained environments. In sum, the Internet of Things is enabling more efficient use of resources, improvements to services and safety, and creating a greater sense of connectedness within emerging smart cities.

The benefits associated with Smart Cities are economic, social, and political, but many of the enablers of these initiatives are technological in nature. According to Goldman Sachs, there are five key technologies driving IoT proliferation which in turn supports Smart City efforts:[18]

- **Cheap bandwidth** The cost of bandwidth has declined precipitously, by a factor of nearly 40X over the past 10 years.

- **Cheap processing** "Moore's law" tells us that over the history of computing hardware, the number of transistors in integrated circuits doubles approximately every two years. Similarly, processing costs have declined by nearly 60X over the past 10 years, enabling more devices to be not just connected, but smart enough to know what to do with all the new data they are generating or receiving.

- **Smartphones** Smartphones are now becoming the personal gateway to the IoT, serving as a remote control or hub for the connected home, connected car, or the health and fitness devices consumers are increasingly starting to wear.

- **Ubiquitous wireless coverage** With Wi-Fi coverage now moving to rapid adoption of 4G

LTE, nearly ubiquitous wireless connectivity is available for free or at a very low cost, given Wi-Fi utilizes unlicensed spectrum and thus does not require monthly access fees to a carrier.

- **Big data** As the IoT will by definition generate voluminous amounts of unstructured data, the availability of cloud/software as a service and big data analytics is a key enabler.

In short, the cost of connectivity has declined while new ways of analyzing large amounts of data have been developed. As a result, governments and companies alike are focused on the IoT as a driver for technological innovation and new capabilities. For example, in 2014 AT&T introduced a Connected Car service in the United States in partnership with several automobile manufacturers, including Audi, GM, Tesla, and Volvo. This service offered high-speed 3G or 4G connections for a monthly subscription fee of $10, thereby enabling vehicles to serve as Wi-Fi hotspots with connectivity for up to seven devices as well as giving them access to OnStar for emergency assistance and remote vehicle diagnostics. By 2015, thirty of GM's models offered this service.[19] In order to improve productivity and save costs, businesses are also embracing the IoT, especially in the areas of labor and energy. For example, in Singapore, the employment of software-defined modular data centers is resulting in operational cost savings of up to 30 percent per enterprise.[20]

A critical part of the story is the expansion of the infrastructure that supports Internet-based communications, including fiber optic cables, satellites, and wireless networks. At the same time, the rapid proliferation of personal electronics devices, sensors, and cloud-based computing infrastructures has given rise to a network of billions of pieces of software and hardware than can now generate, process, and exchange data.[21] Ninety percent of the world's data today has been created in the past two years[22] and that data is now forecasted to double every two years through the year 2020.[23] Combined with global connectivity and big data, the IoT creates concerns about threat vulnerability, overall security, and privacy.

IOT THREATS AND RISKS

According to a report published by the U.S. Federal Trade Commission (FTC) in 2015, IoT devices can be exploited through: (1) unauthorized access and misuse of personal information (e.g., exploitation of personal identity data on a smart TV); (2) attacks on other systems (e.g., cascading Distributed Denial-of-Service (DDOS) attacks through interconnected Point-of-Sale (POS) and Heating Ventilation and Air-Conditioning (HVAC) systems); and (3) safety risks (e.g., automated cars "gone wild").[24] The report further notes that although "each of these risks exists with traditional computers and computer networks, they are heightened with the IoT."[25] A notable example was provided

when two hackers gained access to the control systems of 2014 Jeep Cherokee and disabled its transmission and brakes.[26] As a result, Fiat Chrysler issued an unprecedented recall of 1.4 million vehicles.[27] Medical equipment and devices, such as pacemakers and drug infusion pumps, have also proved susceptible to hacking. In one instance, two patients successfully hacked pain medication drips to increase their dosages.[28] In the words of Wired Magazine: "this year has made clearer than ever before that this Internet of Things introduces all the vulnerabilities of the digital world into our real world. Security researchers exposed holes in everything from Wi-Fi-enabled Barbie dolls to two-ton Jeep Cherokees."[29] Other potential security risks include, but are not limited to, the collection of personal information, locations, habits, and physical conditions.[30]

We are also living in a world where national, provincial, and local governments are critically dependent upon a common, secure financial services framework to conduct the business of the country—services that needs to be available 100 percent of the time. We are moving to a world where citizens in the region and around the globe can only be safe and secure if communities and nations move with knowledge and speed to continually mitigate global risk. To do this, we need both government and industry to effectively use the IoT and big data for innovation and risk mitigation. We need trust!

BUILDING PARTNERSHIPS, BUILDING TRUST

In order to architect and sustain safe, secure smart cities and reap the benefits of the IoT, trust has to be built and maintained among government (including international, federal, state and local levels), commercial companies, and civil society. Any entity working solely for the benefit of itself, or operating in isolation, defeats the very purpose of a Smart City: connecting people and organizations to better the lives of citizens.[31] National governments must take the lead in encouraging public-private partnerships and creating citizen awareness programs to encourage all sectors to move beyond their own operational bubbles to build trust and maintain security in the age of the Internet of Things. There are several notable examples of national governments showing this type of leadership. In the United States, the Department of Transportation has created a Smart City Challenge to spur innovation and promising initiatives in cities across the nation.[32] Numerous countries in Asia, including China, Japan, Korea, and Singapore, are dedicating significant resources to the establishment of Smart City programs. In Europe, a Smart Cities consortium led by the Scottish government is bringing together more than 20 cities from several European countries to enhance city partnerships across the Continent.[33]

PUBLIC-PRIVATE PARTNERSHIP MODELS

While national leadership is essential, at the end of the day, local and regional public-private partnerships are foundational for digitally secure, safe cities. What are the common characteristics of successful public-private partnerships? In our experience, four factors are key:

- **Identification of Government and Industry Champions to Lead and Sustain the Alliance** Government champions are well-suited to be convening authorities and to promulgate standards and policies. Private sector champions are usually the driving force behind financial and human resources.

- **Commitment to Agreed Upon Goals** Successful partnerships also require an unrelenting focus on group goals. These goals must add value to all members of the partnership.

- **Adoption of Common Operating Principles** To promote rapid adoption and scaling, effective partnerships must develop and promote interoperability built upon common standards.

- **Focus on Delivering Enduring Value** Finally, partnerships can be short lived if they become "one trick ponies" especially in the face of an ever changing cyber threat. Available resources will fluctuate as membership and members' priorities evolve. A partnership needs to plan for its complete lifecycle, including sustainment.

The Smart Cities USA program is a good example of a public-private partnership developed and focused on the local level. In this case, the city of San Jose, Calif. is partnering with the Intel Corporation, which is headquartered in the area. Both the city and company have a stake in the outcome since the project could have a positive impact on issues like quality of life, safety, and the cost of living in the area. What's more interesting is that the state of California is partnering with another company, IBM, to create a cloud-based platform that will allow local governments and even other states to access IT resources "while minimizing upfront capital investment and controlling financial risk." Connecting the state and city-level efforts such as these will yield even greater benefits in the development and deployment of secure Smart City projects.

Successful partnerships require unrelenting focus. For organizations like Japan's Computer Emergency Response Team (JP CERT), this unrelenting focus is to develop and deploy world-class computer incident response processes and procedures which

can support Japan's emerging Smart Cities efforts. The JP CERT serves not only the capital and the nation of Japan, but is the executive secretariat across all CERTS for the Asia Pacific (APAC) region. The JP CERT's focus on continuous collaboration and joint computer incident response—tested through rigorous exercises—serves as a role model for other countries hoping to establish national-level incident response centers.

Effective partnerships focus on providing enduring value through continuous innovation in the risk mitigation area. Interpol's Global Center for Innovation (GCI), which is based in Singapore, focuses on cyber forensics, data analytics, capacity building, and proactive security campaigns. In its first year of operation, the GCI has already shown its value in organizing and executing malicious botnet take-downs by working with a wide range of law enforcement organizations across the globe, as well as industry partners. In addition, the GCI works closely with Singapore's government to help improve the cybersecurity posture of the country and support Singapore's massive investments in its Smart Nation initiative.

Although its headquarters is in the United States, the Financial Services' Information Sharing and Analysis Center (FS-ISAC) works with the banks and financial services institutions around the world to improve the exchange of cyber threat information. As nations attempt to ensure that their financial infrastructures are robust in the face of growing cyber threats, FS-ISAC government and industry members will be developing and deploying solutions together. For example, the FS-ISAC and many other information sharing groups are relying on two technological developments that were funded by the U.S. Department of Homeland Security to share cyber threat indicators: the Trusted Automated Exchange of Indicator Information (TAXII) protocol and the Structured Threat Information Expression (STIX™) language.[34]

NEXT STEPS

The incorporation of privacy and security policies and principles and the establishment of public/private partnerships in all smart city projects is pivotal. However, city managers must go beyond plans and take action. An essential element of action is developing relationships with city dwellers on the topics of security and privacy. Mayors and city managers must develop citizen awareness programs concerning the growing digital threat. Beyond awareness and training, city councils and economic development organizations should focus on the establishment of local and regional public-private partnerships and the scaling of existing partnerships. For example, in the Asia-

Pacific region, AP CERT could be empowered to improve computer incident response readiness by collaborating with national capitals in the region on smart city projects. The GCI and its growing partnerships with cybersecurity firms could pilot security data analytics projects for countering cyber crime at the municipal level in the region. Finally, automated cyber threat sharing needs to be adopted as appropriate to bolster the cybersecurity posture of private and public sector organizations. The FS-ISAC model serves as a useful exemplar of how this can be accomplished in large and mature infrastructure sector; other models can be developed to suit the needs of other sectors and regions.

Critical to both government and industry is the ability to measure progress towards the goal of safe and secure smart cities. Fortunately, there are several efforts under way to address this issue. For example, the United Nations has created the United Smart Cities initiative that has several aims, one of which is to establish indicators associated with Smart City outcomes.[35] At the national level, frameworks like the Cyber Readiness Index (CRI) can be used to focus on the security aspects of Smart City deployments. The CRI is a "comprehensive, comparative, experiential methodology to a country's maturity and commitment to securing its national cyber infrastructure."[36] Combining metrics focused on Smart City efficacy and maturity with those that focus on privacy, safety, and security will be an important step in helping governments and companies make good decisions around Smart City deployments.

In sum, city managers, investors, and other city dwellers need to work together to develop and incentivize effective partnerships for secure economic growth. This work includes identifying both government and industry champions, committing to like goals, adopting common operating principles, and focusing on creating enduring value. It is also incumbent on national governments to formulate principles, standards, and norms that stimulate development and growth of the IoT by reducing risk.[37] If they are built on a foundation of trust, Smart Cities have the ability to greatly enhance the quality of life for societies on a local, regional, national, and international level.

Notes

1 “Economy,” UN Habitat for a Better Urban Future, accessed September 3, 2015, http://unhabitat.org/urban-themes/economy/.

2 “Internet of Things – Volume 2; Software and the IoT: Platforms, data, and analytics,” Goldman Sachs Group, Inc.

3 United Nations, Department of Economic and Social Affairs, Population Division (2014). World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352), accessed September 3, 2015, http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf.

4 United Nations, World Urbanization Prospects: The 2014 Revision, Highlights.

5 United Nations, World Urbanization Prospects: The 2014 Revision, Highlights.

6 Karen C. Seto, Burak Guneralp, and Lucy R. Hutyra, “Global forecasts of urban expansion to 2030 and direct impacts on biodiversity and carbon pools.” Proceedings of the National Academy of Sciences of the United States of America. (August 16, 2012), accessed September 3, 2015, http://www.pnas.org/content/109/40/16083.full.

7 “Mobility,” UN Habitat for a Better Urban Future, accessed October 9, 2015, http://unhabitat.org/urban-themes/mobility/.

8 Ibid

9 Clark Gellings, EPRI Fellow and former EPRI VP, presented this information in the spring of 2013.

10 “Safety,” UN Habitat for a Better Urban Future, accessed December 21, 2015, http://unhabitat.org/urban-themes/safety/.

11 “E-Governance and Urban Policy Design,” UN Habitat, accessed December 22, 2015.

12 “Big Data: Seizing Opportunities, Preserving Values,” Executive Office of the President of the United States of America. (May 2014), 2, accessed April 15, 2016, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

13 Joshua New and Daniel Castro, “Why Countries Need National Strategies for the Internet of Things.” (Center for Data Innovation, December 16, 2015), 2.

14 Graph and data: James Manyika, et al., “Unlocking the potential of the Internet of Things.” (2015), accessed February 2, 2016, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

15 “What is a ‘smart city’ and how it will work,” The Times of India (May 2, 2015), accessed April 15, 2016. http://timesofindia.indiatimes.com/What-is-a-smart-city-and-how-it-will-work/listshow/47128930.cms.

16 Ibid

17 José M. Hernández-Muñoz, et al., “Smart Cities at the Forefront of the Future Internet.” (2011), accessed October 9, 2015, http://www.smartsantander.eu/downloads/Presentations/fia_book_2011_smartcities.pdf.

18 “The Internet of Things: Making sense of the next mega-trend,” Goldman Sachs Group, Inc.

19 “The Internet of Things: Making sense of the next mega-trend,” Goldman Sachs Group, Inc.

20 “Adoption of Modular Data Centers to Significantly Bring Down Costs Involved in Setting Up Modern Data Centers by 2019,” Business Wire. (March 3, 2016), accessed March 23, 2016. http://www.businesswire.com/news/home/20160303005048/en/Adoption-Modular-Data-Centers-Significantly-Bring-Costs.

21 “The Internet of Things: Making sense of the next mega-trend,” Goldman Sachs Group, Inc.

22 “Big Data, for better or worse: 90% of world’s data generated over last two years,” Science Daily. (May 22, 2013), accessed February 3, 2016. http://www.sciencedaily.com/releases/2013/05/130522085217.htm.

23 “The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things,” International Data Corporation. (April 2014), accessed February 3, 2016. http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

24 “Internet of Things: Privacy & Security in a Connected World,” Federal Trade Commission Staff Report. (January 2015), ii, accessed April 15, 2016. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

25 Ibid, 10.

26 Andy Greenberg, “Hackers Remotely Kill Jeep on the Highway – With Me In It,” Wired (July 21, 2015), accessed March 21, 2016. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

27 Andy Greenberg and Kim Zetter, “How the Internet of Things Got Hacked,” Wired. (December 28, 2015), accessed February 1, 2016. http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/.

28 James Niccolai, “Thousands of medical devices are vulnerable to hacking, security researchers say,” PCWorld. (September 29, 2015), accessed March 23, 2016. http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html.

29 Andy Greenberg and Kim Zetter.

30 Federal Trade Commission Staff Report, 14.

31 Daniele Loffreda, “Defending the smart City,” Intelligent Utility. (January 5, 2016), accessed February 1, 2016. http://www.intelligentutility.com/article/16/01/defending-smart-city.

32Department of Transportation, Smart City Challenge, accessed August 28, 2016, https://www.transportation.gov/smartcity.

33 Smart Cities Working Together in Europe. July 13, 2016, accessed August 28, 2016, http://oascities.org/smart-cities-working-together-in-europe/.

34For more information, see https://stixproject.github.io/ and https://taxiiproject.github.io/

35 United Nations, United Smart Cities, accessed August 28, 2016, https://sustainabledevelopment.un.org/partnership/?p=10009.

36 Hathaway, Melissa. “Cyber Readiness Index 2.0,” Potomac Institute for Policy Studies. (November 2015), accessed May 4, 2016. http://belfercenter.hks.harvard.edu/files/cyber-readiness-index-2.0-web-2016.pdf.

37 Joshua New and Daniel Castro, 5.