Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Sean Costigan and Gustav Lindstrom,
Connections QJ 15, no. 2 (2016): 9-18
http://dx.doi.org/10.11610/Connections.15.2.01

Research Article

Policy and the Internet of Things

Sean S. Costigan [a] and Gustav Lindstrom [b]

[a] *The New School (link is external), New York, NY, http://www.newschool.edu/*

[b] *Geneva Centre for Security Policy, http://www.gcsp.ch/*

Abstract: Cybersecurity has steadily crept to the top of the national security agenda. Simultaneously, a merger of the physical and virtual worlds is noticeably underway. A confluence of technologies has come together to make this possible under the rubric known as the Internet of Things (IoT). This merger will bring sensors and computing devices totaling in the billions to connect objects together in a network that does not require human intervention, along with which will come much vaunted benefits, knowable risks, uncertainties and considerable security dilemmas. Using the past as a predictor of future behavior, a vast increase in hackable devices will create equally vast vulnerabilities that will now touch the physical world. Yet the IoT will also present opportunities that are just now being imagined, likely making the Internet revolution seem small by comparison. While technological growth often appears to outpace policy, government retains the power to convene and ultimately to regulate. This article examines why policymakers should care about the IoT, the significant trends for the next five to ten years, and likely security implications stemming from those trends. The article finalizes with an overview of policy considerations.

Keywords: Internet of Things, Industrial Internet, security implications of IoT, machine communications, critical infrastructures.

Introduction

Over the past decade, cybersecurity concerns have steadily crept to the top of national and international security agendas. However, with the focus mainly on policies and strategy, rapid technological developments continue to undermine

policymakers' understanding of cyber risks and opportunities. One such development is the Internet of Things (IoT).

While the Internet of Things is not widely discussed among policy circles, it is nonetheless likely to substantially impact how individuals, institutions and societies interact in the future. In brief, the IoT refers to the interconnection of uniquely identifiable, machine-to-machine devices with the Internet. A relatively well-known example from retail industry is the use of radio frequency identification devices (RFID) to track the location of goods and inventory.

According to one estimate, there are currently about 9 billion devices connected to the Internet. This number—which is already greater than the global population—is expected to grow dramatically over the next ten years. According to recent calculations, every second 127 new devices are being added to the Internet.[1] Other projections from notable institutions suggest roughly 50 billion to 1 trillion devices will be connected to the Internet by around 2025, impacting how business is carried out in fields ranging from health care to security policy. This is currently yielding new visions such as the movement to-

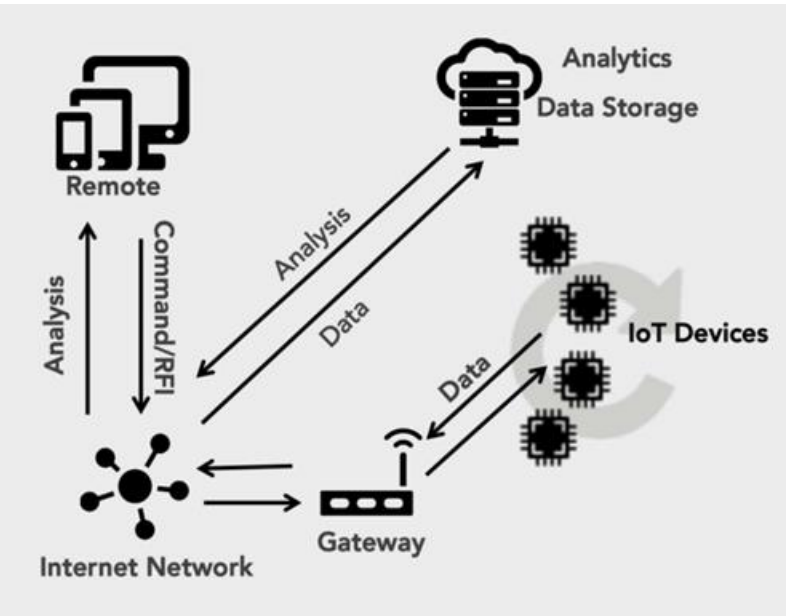

Figure 1: The IoT Ecosystem (Source: Business Insider, www.businessinsider.com).

[1] "127 devices added to the Internet each second, but Congress is clueless about IoT," *NetworkWorld*, 1 July 2015, available at http://www.networkworld.com/article/2942596/microsoft-subnet/127-devices-added-to-the-internet-each-second-but-congress-is-clueless-about-iot.html.

wards as the "Internet of Everything" (Cisco) or the "Industrial Internet" (General Electric). General Electric estimates that the "Industrial Internet" will add $10 to $15 trillion to the global GDP within the next 20 years. With growth of that scale, the IoT is set to usher in a new era of ubiquitous computing that will make the changes brought about by the Internet look small by comparison.

This article examines why policymakers should care about IoT, the significant trends for the next five to ten years, and possible security implications stemming from those trends. The article finalizes with an overview of policy considerations.

Why the Internet of Things Matters

We suggest that there are three main reasons why policymakers should care about the IoT. First, the Internet of Things has the potential to contribute to substantial economic growth. Current developments, such as the gradual introduction of smart meters (for energy efficiency) and driverless vehicles (for transport and logistics) represent just a small sample of the opportunities offered by IoT. Applications are possible in most fields, opening the door to economic growth primarily via efficiency gains and new services that need not entail human intervention. A 2015 study by Accenture suggests IoT can add $10.6 trillion to the cumulative GDP of 20 developed and emerging economies that represent over 75% of the world's economic output.[2] Another report by the McKinsey Global Institute estimates an IoT economic impact of $2.7 to $6.2 trillion annually by 2025.[3]

Second, the IoT will impact diverse and multiple fields, enabling advances and efficiencies across disciplines as opposed to within one or two areas. With this in mind, the areas that are most likely to gain from the IoT are health care, infrastructure, and public sector services.[4] Given current trends, the applications enabled by the IoT will be wide ranging and some cases only limited by imagination. Prospects range from "smart cities" to "personalized healthcare." Specific examples might include a more efficient traffic flow as street signs or stop lights that can communicate with each other and with vehicles in their

[2] Mark Purdy and Ladan Davarzani, "The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity" (Accenture Strategy, 2015), available at https://www.accenture.com/_acnmedia/Accenture/ Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_18/Accenture-Industrial-Internet-Things-Growth-Game-Changer.pdf.

[3] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy," Report (McKinsey Global Institute, May 2013), available at http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies.

[4] For additional information on the economic impact of the IoT see Charles Saidu, Adamu Usman, and Peter Ogedebe, "Internet of Things: Impact on Economy," *British Journal of Mathematics & Computer Science* 7:4 (2015): 241–251.

proximity. IoT sensors can be placed on infrastructures such as bridges to identify micro fissures and cracks, enabling preventative efforts to prolong their lifespan. Within the defense sector, IoT may be used to enhance logistics and transport. IoT may also play a role in autonomous weapons systems, especially as consideration is given to automated systems.

Third, policymakers should care about IoT because there are probable drawbacks and unintended consequences, some of which can have implications for society, critical services and infrastructures. At the minimum, societal dependency on the IoT and a growing "attack surface" will have significant and hard to predict consequences. These issues will be examined in greater depth in the section on potential security implications.

Future IoT trends

Looking ahead, three interrelated trends stand out vis-a-vis the IoT. The first is an accelerating rate of diffusion which, though in its infancy, is already visible today. To illustrate, there was a 30% increase in things connected to the Internet from 2014 to 2015. Table 1 below provides an illustration of projections across different sectors.

Table 1. IoT Diffusion by Sector in Billions of Devices (2015–2020).

Category	2015	2020	Percent Increase
Automotive	372	3511	944 %
Consumer	2,875	13,173	458 %
Generic business	624	5,159	827 %
Vertical business	1,009	3,164	314 %
Total	**4,880**	**25,007**	**512 %**

Source: Gartner, "4.9 Billion Connected 'Things' will be in use in 2015, November 2014.

As shown in the table, the total percentage increase across the four categories examined is approximately 500%, with most growth in IoT diffusion expected in the automotive sector. If these trajectories are even close to accurate, society will be facing substantial changes in how it collects, monitors, and processes information. This trend will be fuelled by two other distinct developments: 1) Continued developments in communications protocols (including wireless), energy storage (e.g. for batteries), microelectromechanical systems (MEMS), and computing power, and 2) Developments in areas that can impact the applicability of IoT such as nanotechnology, artificial intelligence, and data

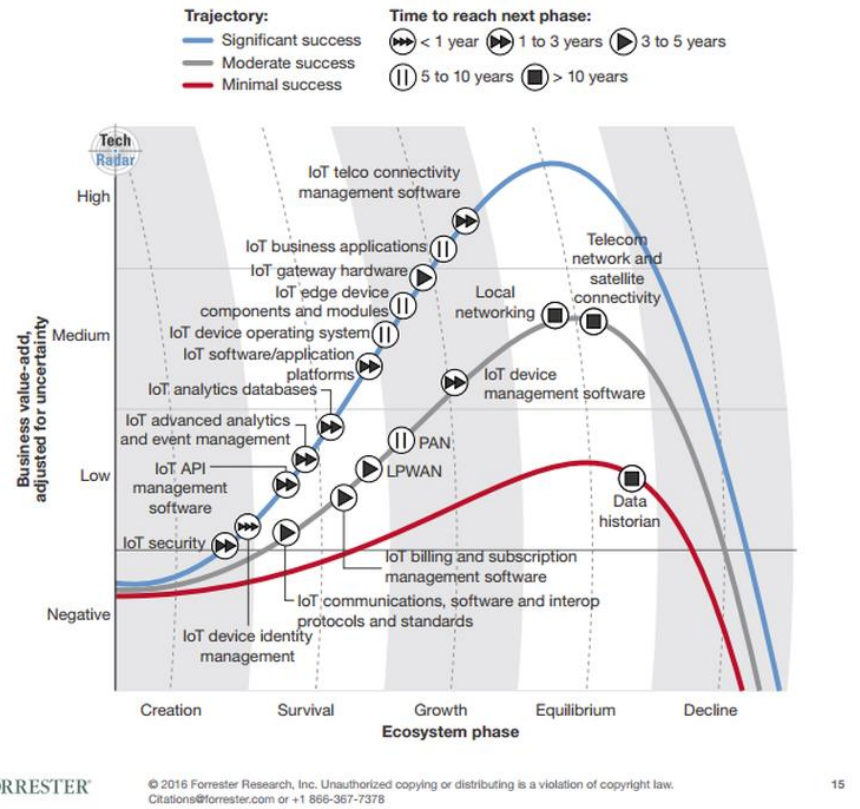

Figure 2: IOT Business Value-Add Over 10 Years
Source: Forrester Research, www.zdnet.com/article/internet-of-things-security-years-away-from-being-fully-baked-says-forrester.

science.[5] Combined, these two will enhance both the reach and applicability of IoT across a variety of sectors.

A second trend is the rapid growth in machine (M2M) communications. As IoT diffusion increases, so will the direct communication between devices that are connected to the Internet, either through wired or wireless form. One estimate forecasts the total number of M2M connection worldwide to increase from roughly 196 million to 361 million in 2018 – an increase of 184% over three years.[6] This trend is significant since we cannot fully predict the consequences stemming from the growth in M2M. In a world were communications

[5] For reference, there are multiple protocols that facilitate communication across devices. These range from wireless protocols such as ZigBee, Bluetooth, and BACnet to developing standards such as RPL, CoAP, and 6LoWPAN.

[6] The Statistics Portal, Statista, 2016. Available at www.statista.com/statistics/295635/total-number-m2m-connections-worldwide.

are between an individual and a device, or between two devices, the outcomes are easier to predict. In an IoT world, data and communications will become ubiquitous.

For example, if a sensor is tasked to monitor the temperature in a location and is programmed to send a warning to an individual or other device when the temperature reaches a certain point, the directionality is clear and simple. With devices increasingly communicating instantaneously while managing or monitoring processes, the relationship becomes multidimensional, complex and possibly more stochastic or random. Given this trend, the ability to control specific relationships between devices may become more complex and unpredictable.

Lastly, growth in IoT and M2M will deliver ever larger amounts of machine-generated data. According to a 2012 IDC Digital Universe study, machine generated data is projected to increase by a factor of 15 by 2020.[7] IDC further notes that about 40% of all data is likely to be machine generated by 2020. This trend will have implications across various areas, specifically on how the data is gathered, processed, stored, and shared. Here, too, policy lags behind.

Potential Security Implications

Two key security implications are likely to arise from the IoT revolution. The first and foremost is addressing the lack of security functions in the majority of sensors and actuators that make up the backbone of the IoT. Specifically, as companies push out more minimally viable products in a rush to meet demand, low-cost sensors and actuators for data collection, monitoring, and process optimization will remain unlikely to have properly embedded security functions within them. Security is apt to remain an expensive afterthought.

Moreover, sensors tend to suffer from limited memory capability and computational power, further diminishing opportunities to produce IoT devices with appropriate security protocols (which frequently is not a primordial goal in the mind of developers). This inherent weakness in IoT translates into possible societal vulnerabilities as devices across sectors ranging from health to agriculture can be compromised.

This IoT vulnerability is already associated with critical infrastructure protection, where there is concern that industrial control systems such as Supervisory Control And Data Acquisition (SCADA) may be compromised in a way that blocks a critical service or infrastructure. With billions of new devices being brought online, the attack surface of modern society will vastly increase, bringing with it the same ever-present vulnerabilities that we see today but at a greater scale. Cascading problems may be more likely, as systems will control other systems. Control systems, which previously were principally accessed via

[7] John Gantz and David Reinsel, "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East" (IDC, December 2012), available at www.emc.com/leadership/digital-universe/2012iview/index.htm.

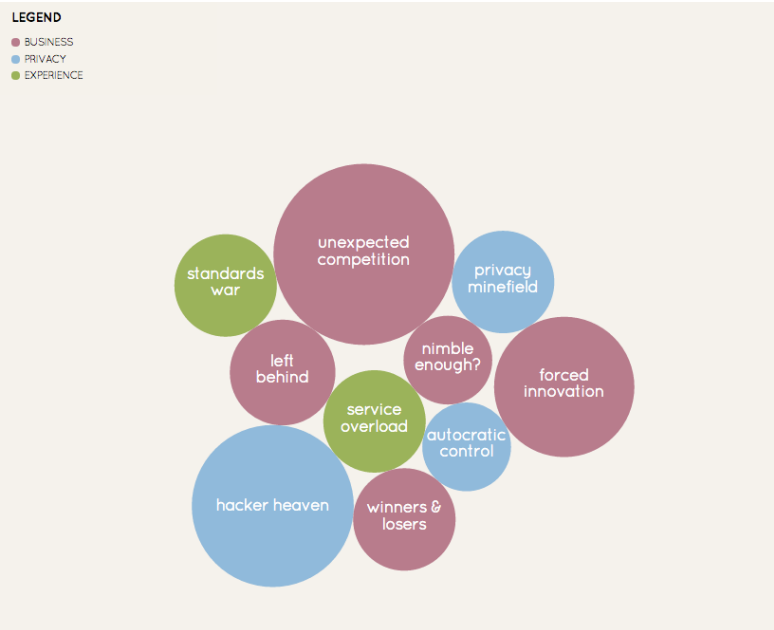

Figure 3: Challenges for the IoT.
Source: Information is Beautiful, http://www.informationisbeautiful.net.

proprietary systems that were not connected to the Internet, are now increasingly accessible through commercial-off the shelf programs that can be accessed online. This vulnerability has gained increased attention after specific attacks on Iran's nuclear centrifuges (via Stuxnet) and Saudi Aramco's workstations (via Shamoon). In short, the IoT is apt to make the Internet even less secure for everyone.

A second challenge posed by IoT is the balance between individual privacy rights and security requirements. As Bruce Schneier recently put it, "surveillance is the business model of the Internet"[8] and that is set to vastly increase in an IoT world. The impact is likely to be underestimated in the short- to medium-term, especially as IoT is combined with developments in other fields. For example, the placement of sensors in clothing materials—facilitated by advances in nanotechnology—opens the door to monitoring information on an individuals' location and possibly some vital signs. Looking ahead, should the use of implanted sensors for monitoring health status become more accepted, it could result in the collection of large-scale data on individuals' health status.

[8] Bruce Schneier, "The Internet of Things Talks About You Behind Your Back," 13 January 2016, available at https://www.schneier.com/blog/archives/2016/01/the_internet_of.html.

This development is already underway with the so-called wearables movement, but once again will be likely to vastly increase in power and diffusion in the next decade. While there could be many benefits from a more personalized health care system, it may also raise challenges with respect to individuals' access to health insurance packages and ability to secure employment opportunities.

The already complex question of balancing privacy and security rights will thus become increasingly thorny. With the prospect of billions of sensors and IoT devices deployed, policymakers will have to more carefully analyze the ways in which data can be compromised. Thus, beyond collection issues, a greater understanding of vulnerabilities at other stages will be needed; for example: how IoT information is collected and used (for example is it shared with third parties?); whether there are risks that sensitive IoT data be accessed by third parties; and how the value of data changes when it is combined with other data.[9]

Policy Considerations

The movement towards the Internet of Things presents several substantive policy considerations for policymakers. The paramount issue is how to best position national policies and strategies to take advantage of IoT benefits while minimizing possible risks associated with more devices connected to the Internet. Precious few countries (such as the Czech Republic, United Kingdom and Australia) and organizations have done such an analysis at the national level, with other countries either adopting a watch and wait approach or none at all.

Second, policymakers should be aware of the chokepoints that might negatively affect the opportunities presented by IoT. Currently, there are a number of outstanding issues that will impact the way IoT evolves, ranging from technical considerations—such as the ability to agree on specific standards for IoT network communication—to strategic considerations regarding the applicability of IoT within the security realm.

Third, policymakers should try to better understand the unintended consequences stemming from the IoT revolution. For example, how might employment and national economies be disrupted as certain skill sets become redundant? From a legal angle, how might the IoT impact laws or regulation safeguards? From a technical perspective, what are implications on divergent views concerning how IoT devices are configured and managed (e.g. should devices announce themselves? How should they be authenticated? Should the IP-addresses for IoT devices be generated automatically or should they be auto generated)? Needless to say, decisions concerning technical arrangements can result in multiple unintended consequences across sectors.

[9] Rolf Weber, "Internet of Things: Privacy Issues Revisited", *Computer Law & Security Review* 31 (2015): 618–627.

Fourth, government should encourage active discussions on embedding security in products. It is increasingly clear that there are limited incentives for IoT device makers to integrate security protocols into their products. On the other hand, it is likewise becoming evident that a lacking or weak security prolife may result in dire consequences. Recent examples include the demonstrated ability to gain access to an aircrafts' velocity and steering functions via the on-board entertainment system,[10] successful attempts to hack IoT enabled medical devices such as insulin pumps,[11] search engines that allow people to peer on unsecured baby cameras,[12] and weaknesses in automobiles and other driverless vehicles.[13] As these vulnerabilities are better known and mapped, the more difficult it will be for industry and policy circles to leave them unattended.

Finally, government retains the power to convene and ultimately to regulate. As such, government has responsibility to stay ahead of the curve on security concerns and has the power to encourage the adoption of new technologies and standards that should produce considerable gains for society. As a starting point to ameliorate the security situation and to improve the adoption of more secure devices, government should fund expert-level research that could be used to initiate a consistent "systems approach" to security and the IoT. Such an approach is apt to pay dividends for decades to come.

[10] Dylan Tweney, "FBI Says This Hacker Took Over a Plane through Its In-flight Entertainment System," *VentureBeat*, 17 May 2015, available at venturebeat.com/2015/05/17/fbi-says-this-hacker-took-over-a-plane-through-its-in-flight-entertainment-system/.

[11] Eric Basu, "Hacking Insulin Pumps and Other Medical Devices," *Forbes*, 13 August 2013, available at www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#2715e4857a0b5822f59f4327.

[12] J.M. Porup, "How to Search the Internet of Things for Photos of Sleeping Babies," *ArsTechnica*, 19 January 2016, available at http://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[13] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It," *Wired*, 21 July 2015, available at http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

About the authors

Sean S. Costigan is a consultant and analyst on technology, risk and security. He is Senior Advisor for Emerging Security Challenges at the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes and Lecturer at The New School, in New York City. He leads a joint NATO/PfPC cybersecurity curriculum development effort for European defense academies. He was recently a member of the Intelligence Community Analyst Private Sector Program for the U.S. Department of Homeland Security and ODNI, and has consulted for the U.S. federal government on information technology, cybersecurity, environmental security and foresight. His latest book *Cyberspaces and Global Affairs* is available in English and Chinese.
E-mail: costigs@newschool.edu

Gustav Lindstrom is the head of the Emerging Security Challenges Program at the Geneva Centre for Security Policy (GCSP). Previously, he headed the GCSP's Euro-Atlantic Security Program and was the Director of the European Training Course. He currently represents the GCSP on the Executive Academic Board of the European Security and Defence College and serves as the co-chair of the PfP-C Emerging Security Challenges Working Group. Dr. Lindstrom received his doctorate in Policy Analysis from the RAND Graduate School and M.A. in International Policy Studies from Stanford University. Prior to his tenure at the GCSP, Dr. Lindstrom served as a Senior Research Fellow at the EU Institute for Security Studies (EUISS). His areas of interest and expertise include European Common Security and Defence Policy (CSDP), emerging security challenges, non-proliferation & disarmament, and cyber security.
E-mail: g.lindstrom@gcsp.ch.