Centre for International
Governance Innovation

Policy Brief No. 160 — July 2020

Standards for Cybersecure IoT Devices: A Way Forward

Michel Girard

Key Points

→ The cybersecurity risks of Internet of Things (IoT) devices are well documented.

→ In the absence of safety and cybersecurity regulations, credible performance standards represent our last line of defence to embed security into IoT devices at the operating level.

→ However, no global standard has been set to address this issue.

→ The growing battle for technological supremacy between the United States and China is partly to blame for the current stalemate in global high-tech standards development.

→ Recent legislative initiatives in the United States could spur the creation of a new regional market for cybersafe IoT devices for the military and for government operations through procurement, as opposed to new regulations.

Introduction

In their drive to digitize their economies and societies, developed countries are making significant investments in big data infrastructure. Over the coming years, billions of additional IoT devices and sensors are slated to come online. These devices will stream data through fifth-generation (5G) networks to cloud-based “data lakes.” IoT-generated data will help train algorithms and allow machine-to-machine systems to operate seamlessly.

However, users now realize that these devices are not designed with cybersecurity in mind. Minimum central processing unit (CPU) and memory capacity are needed for users to manage and maintain IoT devices and keep them cybersafe. The breakneck speed of innovation, the intense competition between vendors to capture new markets and the absence of safety and security regulations with respect to internet-related technologies have contributed to the current situation. As a result, every region of the globe has witnessed IoT cybersecurity breaches, with impacts on products such as self-driving vehicles and medical devices, as well as systems and networks operating critical infrastructure such as military equipment, utilities and telecommunication networks. Although principles to make the IoT more secure have been proposed by a host of organizations in the past three years, no single global standard exists (nor is one under development).

About the Author

Michel Girard is a senior fellow at CIGI, where he contributes expertise in the area of standards for big data and artificial intelligence (AI). His research strives to drive dialogue on what standards are, why they matter in these emerging sectors of the economy, and how to incorporate them into regulatory and procurement frameworks. He highlights issues that should be examined in the design of new technical standards governing big data and AI in order to spur innovation while also respecting privacy, security and ethical considerations.

In addition, Michel provides standardization advice to help innovative companies in their efforts to access international markets. He contributes to the CIO Strategy Council's standardization activities and advises the Chartered Professional Accountants of Canada on data governance issues.

Michel has 22 years of experience as an executive in the public and not-for-profit sectors. Prior to joining CIGI, Michel was vice president, strategy at the Standards Council of Canada (SCC), where he worked from 2009 to 2018. At the SCC, he led the design and implementation of the Standards and Innovation program, the Climate Ready infrastructure program, the Northern Infrastructure Standards Initiative and the Monitoring Standards in Canadian Regulations project. He managed the negotiation of standardization clauses in trade agreements including the Comprehensive Economic and Trade Agreement and the Canadian Free Trade Agreement. Previously, he was director of the Ottawa office at the Canadian Standards Association, director of international affairs at Environment Canada, corporate secretary at Agriculture Canada and acting director of education and compliance at the Canadian Environmental Assessment Agency. He holds a Ph.D. and a master's degree in history from the University of Ottawa.

A Panoply of Devices

The IoT encompasses a wide variety of *internet-ready* devices that do not match the level of sophistication of products such as smartphones, servers or laptops. In its definition of the IoT, the National Institute of Standards and Technology (NIST) includes any device that has at least one *transducer* (either a sensor or an actuator) for interacting with the physical world, and at least one *network interface* (such as Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution or LTE, Zigbee, and Ultra-Wideband or UWB) for interacting with the digital world (NIST 2020, v).

Figure 1 illustrates IoT devices' uses in residential, commercial and industrial settings

IoT devices can be roughly classified into three categories:

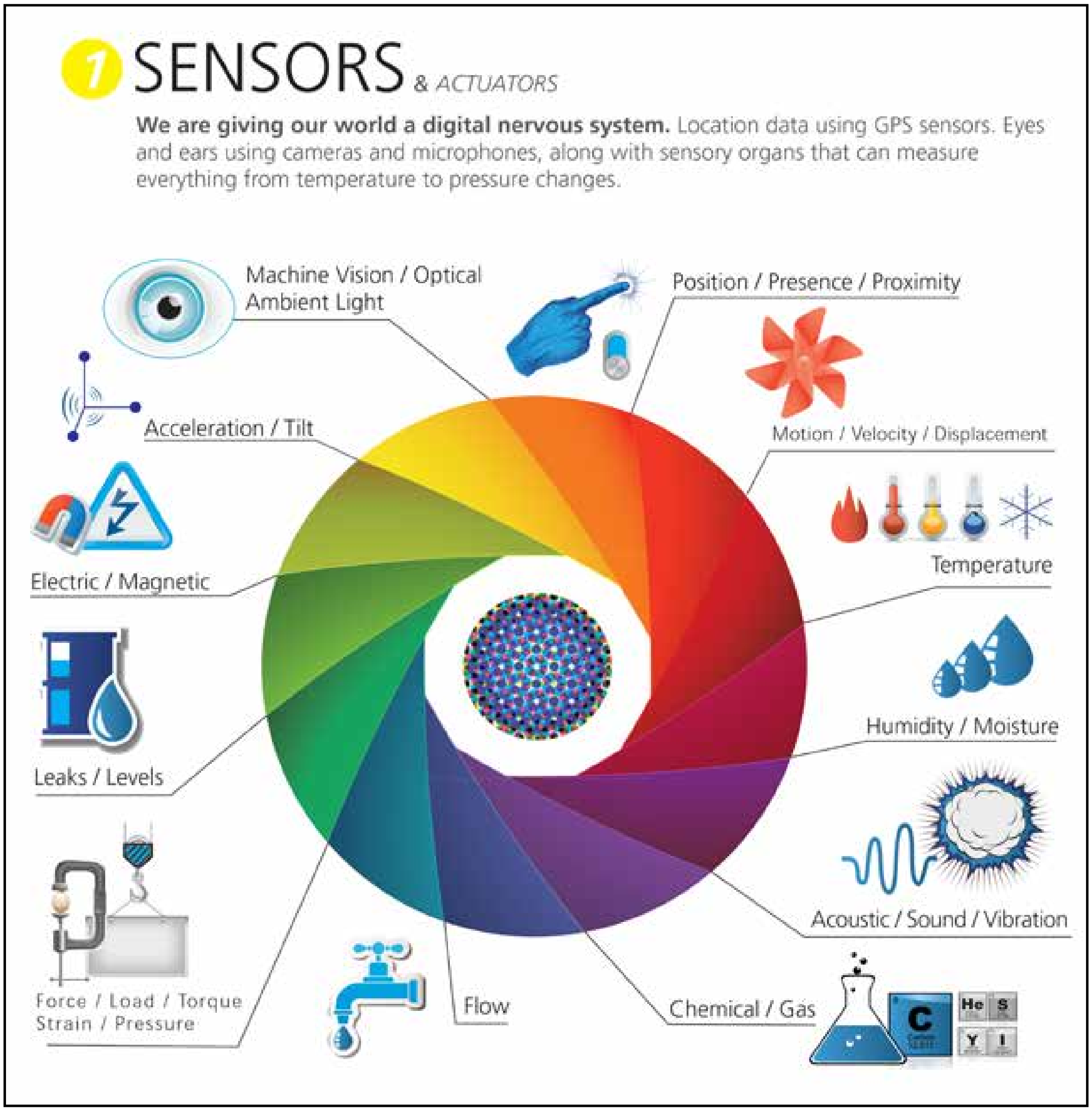
→ Low-end IoT technologies that provide data: These devices are relatively simple and low-cost, such as sensors that transmit information one way. Examples include sensors used for security that indicate whether a window or door is open or closed.

→ Mid-level IoT technologies that provide both data and functionality: These devices have data-processing capabilities, may send and receive data, or could have some actuation functionalities. Examples include sensors that trigger valves once temperature or pressure reaches a certain threshold or that communicate actions to operators.

→ High-end IoT technology that provide data, functionality and control: These devices, such as self-driving cars, perform high-value functions and require high amounts of bandwidth (Rauscher 2019, 8–11).

Depending on the definition being used, there were between eight and 15 billion devices connected to the internet in 2015. Estimates for 2020 range from between 25 and 30 billion devices. Looking ahead, the number of connected devices could range from between 50 and 75 billion devices by 2025 and could continue to increase thereafter (Yoo 2019, 41; Hidden Brains 2020; US Senate 2019, 2). This growth in IoT is generating large data flows. Although traditional data centre traffic was expected to triple between 2017 and 2020 to 15.3 zettabytes (ZB), IoT

Figure 1: IoT Devices — Sensors and Actuators


1
SENSORS
& ACTUATORS
We are giving our world a digital nervous system. Location data using GPS sensors. Eyes and ears using cameras and microphones, along with sensory organs that can measure everything from temperature to pressure changes.
Machine Vision / Optical
Ambient Light
Position / Presence / Proximity
Acceleration / Tilt
Motion / Velocity / Displacement
Electric / Magnetic
Temperature
Leaks / Levels
Humidity / Moisture
Acoustic / Sound / Vibration
Force / Load / Torque
Strain / Pressure
Flow
Chemical / Gas
C
He
S
Y
I

Source: Reproduced with permission from Postscapes and Harbor Research, www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/.

growth over the same period was forecasted to be 39 times higher and to reach 600 ZB (Keeley 2017).

The economic value of the sector is large and growing. According to research firm Gartner, total global expenditure on IoT is set to top US$3 trillion this year. Although future prospects vary, research firm McKinsey estimates that the economic value of IoT across sectors could reach US$11 trillion per year by 2025, depending on factors such as the extent of the deployment of 5G technologies globally (Groupe Spécial Mobile Association [GSMA] 2018, 15). The IoT could spawn hundreds of new billion-dollar-plus unicorns as all sectors of the economy turn to digitization (Rauscher 2019, 16).

5G Interoperability and Cybersecurity Standards

It should be noted, however, that these estimates are all contingent on two factors related to standardization that are critical for success. The first factor is the ability to achieve interoperability between devices and networks. Although an important bottleneck to the deployment of IoT devices was removed with the adoption of Internet Protocol (IP) version 6 to deal with the looming IP address exhaustion issue, both developers and users agree that the industry as a whole needs to make significant progress on establishing appropriate interoperability standards for data to flow freely from IoT devices to 5G networks and then to platforms (SOS International [SOSi] 2018, 3; GSMA 2018, 15). However, given the growing competition for technology supremacy between the United States and China, progress on many important global standards has stalled in the United States in the face of significant progress in China, notably when it comes to the development of global interoperability standards. There is a generalized perception that US industry participation in global voluntary standards setting related to 5G and related technologies has declined over the years, in particular at the International Telecommunication Union (ITU) (SOSi 2018). US industry participation has been further restricted across voluntary standards-setting bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) since May 2019 when the US Department of Commerce added China's Huawei to its export control regulation Entity List (Rubio 2020). This decision has since been reversed in June of 2020. Without significant progress on the standards front, interoperability will remain elusive for US-backed technologies, and the deployment of US-sanctioned 5G technologies will be delayed.

Not Designed with Security in Mind

The other significant barrier to widespread adoption of the IoT is the absence of cybersecurity standards that apply to IoT devices per se. Since the commercial deployment of devices a little more than 10 years ago, the IoT has been the target of a wide array of cybersecurity breaches. A growing percentage of cyberattacks featuring viruses, worms, trojans and botnets are being introduced through unsecured IoT devices. In 2017, 48 percent of US companies with IoT devices on their network had experienced a breach (Businesswire 2017). That percentage is bound to rise further with the introduction of more devices. According to industry experts, approximately 25 percent of all cyberattacks will target IoT devices in 2020 (Toomey 2018).

Regarding botnets, millions of unsecured IoT devices have reportedly been used to launch denial of service attacks (DDoS), including the 2016 Mirai attack, which represented the largest DDoS attack on the internet at the time (Holland 2019, 52). Newer iterations of IoT-focused attacks, such as Hajime and Devil's Ivy, can identify different devices, select known passwords or exploit appropriate vulnerabilities, compromise a device and then use its communications protocols to spread infection to other devices. According to Anthony Giandomenico (2017), an expert on the IoT, "the potential for using multi-vector worms to create massive IoT botnets that span across multiple technologies is very real. And the results can be devastating."

Nation-states are also directing and funding research aimed at identifying IoT cyber vulnerabilities. According to SOSi (2018, 109–11), the China National Knowledge Infrastructure database listed 1,229 published articles on IoT security in July 2017, including articles on the development of algorithmic and machine-learning techniques for the systematic discovery of IoT vulnerabilities across a wide range of devices around the world.

The potential for serious harm or even death for users now appears to be higher with unsecured IoT devices than with any other consumer good. Erroneous information can be introduced in industrial sensors and trigger incidents, accidents or shutdowns. IoT devices installed in appliances, home automation products, cameras and laser printers are used by unauthorized third parties to access household, commercial and industrial networks (Constantine 2015). Wind farms can be disabled (Greenberg 2018). Individuals or groups can be targeted and killed through intrusion in IoT devices operating the driving functions of cars, pacemakers or insulin pumps. Appliances can self-destruct though the tampering of sensors and actuators. Exploding pieces of equipment can maim or kill (Yoo 2018, 43; Hunt, Letey and Nightingale 2017, 1).

The main reason why IoT devices are vulnerable is because there is not enough CPU and memory embedded in them to allow users to manage them by updating software, adding unique identifiers or new coding or patches. The circuit board space is too small to accommodate the required security and authentication protocols. Often, the software embedded in the device cannot be accessed under current configurations, updated or patched (Maddison 2019). According to IoT industry specialists, manufacturers have an important role to play in enhancing the resilience of the devices they produce, but they have not prioritized security to date, "mostly because they are motivated by profit; they want to bring as many of these devices to market as quickly and as cheaply as possible" (Toomey 2018). Insufficient investments in the security needs of these and other price-sensitive devices have left consumers and society critically exposed to device security and privacy failures (Hunt, Letey and Nightingale 2017, 1).

This situation has generated a number of responses. On the one hand, it has fostered the creation of a cottage industry of firms focusing on network and system cybersecurity advances to shield IoT devices from attack. Websites such as Shodan serve as a meeting place to identify, showcase and address — or, in some cases, allow malicious actors to take advantage of — IoT vulnerabilities through comprehensive databases.[1] The Department of Homeland Security maintains a dedicated and ever-expanding webpage focusing on IoT devices advisories to alert critical infrastructure operators as weaknesses are discovered.[2]

On the standards front, however, no discernible progress has been made in developing global cybersecurity standards focusing squarely on IoT devices. Standards bodies such as the ISO/IEC, the Institute of Electrical and Electronics Engineers (IEEE), the ITU and the Internet Engineering Task Force have published a wide range of cybersecurity standards and guidance focusing on networks, systems, processes, controls and vulnerabilities (SOSi 2018, 50-51). In the United States, NIST has also published cybersecurity guidance in its 800 series and in its Federal Information Processing Standards series. Underwriters Laboratories (UL) has been able to partially fill the gap through its UL 2900 Standard for Software Cybersecurity for Network-Connectable Products. However, the standard, as stated in its title, does not contain minimal requirements on hardware contained in the devices (UL 2017).

In the past three years, there has been a growing interest in exploring new approaches. On the industry side, 12 US and European organizations representing developers, vendors and users issued detailed guidance to improve the cyberperformance of IoT devices. These documents are detailed enough to be used as seed documents for future standards.[3] Governments have started to take steps to manage this space as well. In September 2018, California passed the Security of Connected Devices Act, which codifies the state's ability to bring enforcement complaints against companies that do not build adequate security safeguards into their devices. In September 2019, the US Senate Committee on Homeland Security and Governmental Affairs reviewed Bill S.734 on the Internet of Things Cybersecurity Act and requested that NIST develop standards featuring minimum security requirements for IoT devices that would be procured by federal agencies, thereby creating a market for cybersafe IoT devices.

NIST Recommendations for IoT Device Manufacturers

In response to the Senate Committee, NIST issued draft recommendations for IoT devices' cybersecurity to manufacturers in 2019. A second, more comprehensive draft was released in January 2020. Although it clearly states that IoT devices "often lack device cybersecurity capabilities their

[1] See www.shodan.io/.

[2] See www.us-cert.gov/ics.

[3] Detailed guidance on core device cybersecurity capabilities for IoT devices has been submitted by the Agelight Digital Trust Advisory Group; the Broadband Internet Technical Advisory Group (BITAG); the Cloud Security Alliance; the Council to Secure the Digital Economy; CTIA; the European Union Agency for Network and Information Security; the European Telecommunication Standards Institute; the GSMA; the IEC; the Industrial Internet Consortium; the IoT Security Foundation; the ISO/Online Trust Alliance and the Platform Security Architecture.

Table 1: Measure and Components of Digital Preparedness Index

Device Capability	Objective
Device identification	The IoT device can be uniquely identified logically and physically.
Device configuration	The configuration of the IoT device's software and firmware can be changed, and such changes can be performed by authorized entities only.
Data protection	The IoT device can protect the data it stores/transmits from unauthorized access and modification.
Logical access to interfaces	The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
Software and firmware update	The IoT device's software and firmware can be updated only by authorized entities using a secure and configurable mechanism.
Cybersecurity state awareness	The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

Source: NIST (2020).

customers — organizations and individuals — can use to help mitigate their cybersecurity risks" (NIST 2020, ii), the document does not codify performance requirements that manufacturers can use to test and, more importantly, certify compliant devices. Rather, it provides guidance for manufacturers to engage in a dialogue with customers, and to respond to their cybersecurity needs on a case-by-case basis. Nevertheless, the document proposes six categories of capabilities that could lend themselves to the creation of a credible performance standard. These capabilities, shown in Table 1, are extracted from 12 reference documents produced by industry consortia and published standards.

Although Bill S.734 has not been adopted by Congress, the United States and other jurisdictions can now mandate that new IoT devices purchased by governments and their military adhere to the principle outlined in the NIST document, thereby creating a market in absence of regulation. Embedding the NIST requirements in a performance standard would allow for the creation of an independent third-party certification program for devices and the use of certification marks on products that have met the standard. This approach is supported by those in the industry who are arguing for cybersecurity principles applying to IoT devices, such as the BITAG (BITAG 2016, vi).

The Microsoft-MediaTek Use Case

One of the criticisms of applying a standard and certification program to the IoT is that adding CPU power, memory and software will drive up the cost of devices and reduce the future growth opportunities of the industry as a whole. This argument has been largely debunked by a use case spearheaded by the Microsoft Research and NExT Operating Systems Technologies Group. In an article entitled "The Seven Properties of Highly Secure Devices," the authors of the project argue it is "within the reach of achievability for all devices, even the most price sensitive, to be engineered with sufficient security to be trustworthy even in the face of aggressive assault from determined network attackers." The NExT team partnered with Taiwan-based IoT device manufacturer MediaTek to apply to exisiting devices cybersecurity performance requirements similar to those proposed by NIST. They designed, created and tested Sopris, "a proof of concept highly secure microcontroller" and demonstrated that it is possible to construct a microcontroller that can readily provide the basis for highly secure IoT devices (Hunt, Letey and Nightingale 2017).

Next Steps

In the absence of broad-based regulations setting the bar for minimum cybersecurity features for IoT devices, standards and certification represent the last line of defence to protect consumers, governments, industry and critical infrastructure from cybercriminals and state-sponsored cyberattacks. Bill S.734 and the resultant NIST guidance have created an incentive, a market and sound principles for the development of a credible standard. Looking forward, it is becoming increasingly clear that such a standard would have to be applied to all IoT devices being deployed in the marketplace. Given the growing threats of DDoS events and the possibility of assassination attacks by IoT devices, the health and safety risks are too high to justify exemptions. IoT industry expert Matt Toomey (2018) recently stated: "Hopefully some type of universal security standards can be implemented sooner rather than later. However, if history is any indication, it will probably take more catastrophes to inspire any meaningful progress to be made."

The challenge before us is to find the right standards development body to take on this work. As explained in the 2019 CIGI paper entitled *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter* (Girard 2019), the information and communications technology sector as a whole has shunned global standards development organizations over the past decades, which has created a vacuum in the development of appropriate health, safety and security guardrails to frame big data value chains and their associated hardware, software and policies. A new approach is therefore needed to spur the development of credible cybersecurity standards for IoT devices. Given its neutral position, Canada is ideally positioned to take a leading role. Accredited standards development organizations such as the CIO Strategy Council can offer a neutral ground where cybersecurity specialists, industry and regulators from like-minded jurisdictions can establish trust and achieve results for the benefit of consumers — first by developing a solid standard applicable in Canada, and then by submitting it as an international standard through an established global standards body such as the IEEE or the IEC.

Acronyms and Abbreviations

5G	fifth-generation
BITAG	Broadband Internet Technical Advisory Group
DDoS	denial of service attacks
CPU	central processing unit
GSMA	Groupe Spécial Mobile Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
SOSi	SOS International
UL	Underwriters Laboratories
ZB	zettabytes

Works Cited

BITAG. 2016. *Internet of Things (IoT) Security and Privacy Recommendations*. November. Denver, CO: BITAG.

Businesswire. 2017. "Survey: Nearly Half of U.S. Firms Using Internet of Things Hit By Security Breaches." Businesswire, June 1. www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security.

Constantine, Lucian. 2015. "Researchers: IoT devices are not designed with security in mind." Infoworld, April 7. www.infoworld.com/article/2906641/researchers-iot-devices-are-not-designed-with-security-in-mind.html.

Giandomenico, Anthony. 2017. "For cybercriminals, IoT devices are big business." IoT Agenda, August 10. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/For-cybercriminals-IoT-devices-are-big-business-part-one.

Girard, Michel. 2019. *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter*. CIGI Paper No. 209. Waterloo, ON: CIGI. www.cigionline.org/publications/big-data-analytics-need-standards-thrive-what-standards-are-and-why-they-matter.

Greenberg, Andrew. 2018. "Researchers Found They Could Hack Entire Wind Farms." *Wired*, June 28. www.wired.com/story/wind-turbine-hack/.

GSMA. 2018. "How Greater China Is Set to Lead the Global Industrial IoT Market." www.gsma.com/iot/wp-content/uploads/2018/06/GSMA_Report-How_Greater_China_Is_Set_To_Lead_Global_Industrial_IoT_Market-en-July2018.pdf.

Hidden Brains. 2019. "IoT in 2020: The Market to See a Gigantic Growth in Future — Infographic." November 11. www.hiddenbrains.com/blog/iot-2020-market-see-gigantic-growth-future-infographic.html.

Holland, Bryon. 2019. "TLD Operator Perspective on the Changing Cybersecurity Landscape." In *Governing Cyberspace during a Crisis in Trust*, 49–54. Waterloo, ON: CIGI.

Hunt, Galen, George Letey and Edmund B. Nightingale. 2017. "The Seven Properties of Highly Secure Devices." Microsoft Research NExT Operating Systems Technology Group. www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf.

Keeley, Phil. 2017. "Understanding the Explosion of IoT and Its Impact." *Fortinet* (blog), October 10. www.fortinet.com/blog/industry-trends/understanding-the-explosion-of-iot-and-its-impact.html.

Maddison, John. 2019. "Securing the IoT Edge." *IoT Agenda* (blog), April 15. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda Securing-the-IoT-edge.

NIST. 2020. "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline." Draft (2nd) NISTIR 8259. Washington, DC: US Department of Commerce.

Rauscher, Karl Frederick. 2019. "United States-China Collaboration on the Internet of Things Safety: What Next?" Washington, DC: Atlantic Council.

Rubio, Marco. 2020. "Rubio Joins Colleagues in Urging Administration to Issue 5G Regulations." Press Release, April 14. www.rubio.senate.gov/public/index.cfm/press-releases?ContentRecord_id=423B6F3E-5BCF-4BDE-88CD-25FD45145D4B.

SOSi. 2018. *China's Internet of Things*. Research Report Prepared on Behalf of the US-China Economic and Security Review Commission. October. Vienna, VA: SOSi.

Toomey, Matt. 2018. "IoT Devices Security Seriously Neglected." Technopreneurph, February 13. https://technopreneurph.wordpress.com/2018/02/13/iot-device-security-is-being-seriously-neglected-by-matt-toomey/.

UL. 2017. "Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements." https://standardscatalog.ul.com/standards/en/standard_2900-1_1.

US Senate. 2019. "Internet of Things Cybersecurity Improvement Act: Report of the Committee on Homeland Security and Governmental Affairs to Accompany S.734." September 23. Washington, DC: US Government Publishing Office.

Yoo, Christopher, S. 2019. "The Emerging Internet of Things: Opportunities and Challenges for Privacy and Security." In *Governing in Cyberspace during a Crisis in Trust*, 41–44. Waterloo, ON: CIGI.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Director, Digital Economy Research Robert Fay
Program Manager Heather McNorgan
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org