CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Diverse and Vulnerable: Disconnects in Cyber-security Governance of IoT

by Kristen Csenkey

June 2022

POLICY PERSPECTIVE

DIVERSE AND VULNERABLE:
DISCONNECTS IN CYBER-SECURITY GOVERNANCE OF IOT

by Kristen Csenkey

CGAI Fellow
June 2022

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-249-7

The Internet of Things (IoT) is not new – it's been a part of our daily lives for many years.[1] What is new is the acceleration of digitization and transformation of services, devices and information brought about by the COVID-19 pandemic and their linkages to IoT. Specific devices and technologies, or "things," are connected to networks, systems, infrastructures and humans in different ways for various purposes. Some of these technologies are low-cost to create, while others like vehicles, are a part of a multi-billion dollar market with linkages that span sectors. The increased digitization of our lives brought about during the pandemic has taken us closer and made us more integrated into a cyber-physical world. This increased integration has socio-technical dimensions with connection points across national borders. It also creates new and amplifies existing cyber-security challenges in addition to creating connected and increasingly vulnerable threat environments for malicious actors to exploit.

With an apparent return to great-power competition and increased emphasis on the role of technology in geostrategic competition in the narrative, Canada's capabilities are frequently brought into question. The governance of technologies and connected systems requires a more nuanced understanding, especially one that accounts for the assemblages of interactions between devices and users in addition to their links across sectors and context. Co-operation and collaboration with multiple stakeholders on standardization and regulation is an important part of addressing cyber-security challenges associated with these interlinked technologies. Within the Canadian security policy landscape, this co-operation lacks overall cohesion. Importantly, it lacks the opportunity for international co-operation with trusted partners.

Policy Context

Strong, Secure, Engaged (SSE), Canada's defence policy, recognized the dynamics of the threat environment when it was published in 2017. The environment still includes network and connected technologies, like autonomous vehicles, and the associated cyber-threats. The National Cyber Security Strategy set the tone for Canada's understanding and addressing cyber-threats, with Budget 2018 actioning items such as the Canadian Centre for Cyber Security (CCCS). Budget 2022 announced a defence policy review as an update to SSE with a focus on reinforcing defence priorities to meet ongoing global challenges. Funding for bolstering capabilities, continued contribution to core alliances and reinforcing cyber-security were listed as key priority areas.

When the National Cyber Security Strategy was released in 2018, it estimated there would be over 25 billion connected devices within the IoT ecosystem by 2020. Around 29 billion connected devices are forecast for 2022, with 18 billion related to IoT. Other estimates suggest that by 2025, 75 billion devices will be connected within the IoT ecosystem – and associated with a market value in the trillions. Connected devices and their linkages within IoT to other technologies, people,

[1] There is debate about when exactly the concept of IoT was created and the appearance of the first truly connected device, but generally "things" connected to the internet has been a well-known concept since the early 1990s.

data and networks, exist beyond borders and within multiple and overlapping sectors. For example, transportation, energy, government and defence, among other areas, all have connections, not only through the technologies used therein, but through actors such as individuals, private companies and services, among other links.

Take the automotive and transportation sector, for example, where vehicles at various levels of connectivity interact using sensors and other equipment to understand their environment (including other devices, vehicles, people, infrastructures, etc.) and then communicate this information to other devices. This could include public transit buses, individual cars and fleet trucks, but also in a defence context with military vehicles, including autonomous or automated, but still connected within specific IoT systems.

There are cyber-security concerns for these connected devices within IoT systems regardless of the sector. Transport Canada offers a cyber-security self-assessment tool for all vehicle types with different levels of connectivity, but this assessment is voluntary. In addition, Canada's Vehicle Cyber Security Guidance and Transport Canada's Vehicle Cyber Security Strategy provide a foundational policy focus and goals in understanding the complexities of the connected-vehicle cyber-security threat landscape. Yet, no specific high-level IoT defence policy or regulations exist for ensuring cyber-security of the IoT environment in Canada.

A Connected and Vulnerable Threat Environment

The pandemic brought about many challenges and changes in our daily lives. The increased digitization of many services and activities also brought about new vulnerabilities as more users, devices and information are connected through the internet. These connections are increasingly linked within the IoT environment or ecosystem, where technologies and humans interact. These "things" comprise the modern threat environment where malicious cyber-activities can occur. Malicious actors can access and attack their targets via a threat surface, and generally, the threat surface is expanded when more devices are connected to the internet. Threats and threat actors are multiple, with an impact that goes beyond one domain of focus.

Cyber-threats can come from a variety of actors with malicious intent: private companies, states, criminal organizations, terrorist groups, state-sponsored groups, individuals, automated technologies and other non-human entities,[2] among others. These actors can work in mixed groups, as proxies or as individuals, as well as have different and sometimes overlapping intents, including profit, violence or harm, etc. There are also different motivations, from financial and political, to thrill seeking and other reasons and agendas, including espionage, intelligence gathering or intellectual property (IP) theft. There are also different levels of sophistication of attacks; some require access to advanced technological capabilities, such as to a quantum computer (QC). In an attack using a QC, a potential threat actor would need the ability and

[2] For an interesting map of non-human attackers (without malicious intent), see: https://cybersquirrel1.com/.

finances to build and run a QC; however, only a few states and private sector companies would have the ability to launch a sophisticated attack.

As tempting as it is to simplify, a one-size-fits-all approach to addressing these threats is not the best option. Solutions to address these varying threats may not be appropriate in each context, have interests aligned or have the same accountability requirements. One example that illustrates the complexities involved in understanding, identifying and co-operating to address threats is the increasing interconnection of everyday devices – and this will increasingly include autonomous, automated, remote and connected vehicles. Communication between these devices is a central part of their interactions with other technologies, humans and systems in cyber-physical worlds.

In Focus: IoT and V2X

IoT connects many devices in cyber-physical systems via the internet, linking technologies, humans, data and infrastructures, while blurring lines and pushing the limits of traditional frameworks of defence, security, safety and governance. Technologies, such as autonomous and remote vehicles, are also connected within these systems and to other devices through vehicle-to-everything (V2X) services and play an important role in connecting users and sectors, but also create cyber-security challenges.

Simply, in order to ensure safety of transport, vehicles need to connect to other technologies and communicate with other vehicles to co-ordinate movements – to avoid collisions, for example. We can think of connected vehicles as similar to data centres on wheels, in the sense that they hold a variety of information about the technology and users. V2V communication needs to be secure to ensure that sensitive information remains secure throughout the life cycle of the vehicle and its use on roads and to receive updates. Yet, this security will no longer be assured because the classical cryptography used in V2V communications will be broken by attackers with access to a QC in the near future. Also, there is currently no standard post-quantum (PQ) algorithm that can modify the current V2V communication standards to prevent against attacks. A cyber-attack in this situation could take the form of malicious messages inserted into the V2V communications, making it difficult for vehicles to see or detect other drivers, pedestrians, etc. This could potentially cause serious harm to all "things" connected within the IoT and V2X systems. A switch to more secure cryptographic algorithms will secure against the approaching quantum threat, but currently, compatibility and interoperability are in their infancy. Multiple threats are apparent within the IoT ecosystem and broadly, we can understand them as the challenge of heterogeneity.

The Challenge of Heterogeneity

Diversity is inherent in IoT in the many ways that different devices interact with each other and with users, and how they exist in the cyber-physical world. IoT is in itself diverse and matured with multiple "flavours." For example, there is IoMT (Internet of Medical Things), IIoT (Industrial

Internet of Things) and AIoT (Artificial Intelligence of Things). V2X is also diverse, with technology covering V2V (as previously described), V2I (vehicle-to-infrastructure), V2N (vehicle-to-network), V2P (vehicle-to-pedestrian) and V2R (vehicle-to-roadside unit), among others. Changing behaviours, demands and services during the COVID-19 pandemic may have contributed to the proliferation of the diversity of IoT and of V2V as well as to the capabilities of connected devices. These connected devices have different cyber-security challenges and one is their heterogeneity. There are a number of ways in which heterogeneity is apparent in IoT ecosystems: between users and sectors, and ownership differences.

Devices have multiple uses and these can differ from the original intended ones. These uses may go beyond the manufacturer's expectations and therefore create future and unanticipated vulnerabilities. In addition, not all devices are used the same way in each sector within the IoT ecosystem, but they may link sectors through users. For example, connected vehicles may be used to transport individuals, but also food, medical equipment (including vaccines) and goods delivery in (smart) cities, or logistics and other operational purposes in conflict settings.

Data are generated and collected as linked devices connect with each other in other sectors. The data generated by these linked devices are diverse and not necessarily owned by a single company or by the user. Data may be sent from one device and aggregated in another device; for example, in a cloud system, and used to make decisions and monitor and track things, people and processes. Devices, data and users will and are increasingly connected, and it is important to ensure that they are secure in their interactions in the IoT ecosystem.

Technologies, systems, users, architectures and configurations have different associated cyber-security risks. Ensuring interoperability, identifying the common purposes and adapting to different adoption rates of digitization are additional challenge areas. The governance of these connected technologies, users, data and their convergences between different sectors, including managing threats, requires multi-stakeholder collaboration to ensure a secure IoT environment in the future.

Recommendations for Policy-Makers

Outlining the possible threats and threat vectors within the cyber-environment is one part of ensuring cyber-security of the IoT ecosystem. Drawing awareness to these threats through assessments and public announcements[3] is an important part of filling gaps in knowledge, but it needs to go further. This is because threats are not always understood in the same way by all stakeholders and actors need to be held accountable for preventing and addressing threats.

Mismatched perceptions about the reality of threats can contribute to this misunderstanding and may occur between policy and technical experts in the cyber-security community. To address this,

[3] The Canadian Centre for Cyber Security (CCCS), as part of the Communication Security Establishment (CSE), provides reports and guidance on cyber-threats, including for IoT. For example, IoT security for small and medium-sized organizations and a Get Cyber Safe #IoTatWork campaign and toolkit for SMEs.

more collaboration and communication on threats are necessary to fully appreciate their nuances. Specific IoT cyber-security guidance is needed for device manufacturers, in both technical and non-technical language. There must be broader conversations through consultations with diverse stakeholders about the risks, lived realities and best practices that are considered in policy and implemented in regulation.

Yet, cyber-security policy and regulation alone are not the answers. Broad policy that generalizes threats and puts sweeping requirements into place as solutions to cyber-security challenges may not be a best practice. This is because the diversity of devices, their uses and cyber-security challenges need nuanced responses. This is not to say that policy and regulation are not important. They are very important, but they need to recognize the sectoral differences in cyber-security needs to effectively address risks. A combination of technical and non-technical guidelines and requirements may be a useful way to address cyber-security risks without oversimplifying the diversity of challenges, as well as hold key actors accountable. For example, the U.K., through the Department of Digital, Culture, Media and Sport (DCMS) has recently explored instituting a code of practice for IoT security in consultation with academic and private sector stakeholders, in addition to device-specific guidance. Although Canada, through the Office of the Privacy Commissioner (OPC), released privacy guidance for manufacturers of IoT devices, it was aimed at ensuring compliance with the principles of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In addition, Innovation, Science and Economic Development (ISED) launched a public consultation on IoT and AI, but this was in the context of understanding how these technologies pose challenges to Canada's copyright framework and additional measures for modernization of the *Copyright Act*.

Implications for Canada

In sum, cyber-security threats are broad and multi-domain as are the technologies used therein. The increased connectivity and the interdependencies of technologies, users, processes, etc. may lead to increased vulnerabilities within digital and physical-digital systems by creating more attack surfaces for potential malicious actors with diverse motivations and agendas. There are different uses and concerns relating to cyber-security threats based on the context of use and the role of users. Although threat assessments and raising awareness are an important part of cyber-security, they should be combined with other initiatives, specifically ones that recognize the lived realities and daily uses of the systems and technologies,[4] while holding key actors accountable to ensure cyber-security from the start.

Generally, connected devices are not always built with security in mind. Instead, security should be a starting point by design and not an afterthought where resources are constantly allocated to address vulnerabilities and exploitation. Regulation and standardization are part of a baked-in cyber-security, not only to ensure interoperability of diverse devices, but ongoing collaboration with stakeholders and experts. For example, the U.S. National Institute for Standards and

[4] Based on recent recommendations made for critical infrastructure operators and policy-makers.

Technology's (NIST) Cybersecurity for the Internet of Things program makes specific recommendations for connected devices to meet certain security standards. NIST relies on consultations with experts in industry and academia, as well as user feedback to improve security standards. The European Telecommunications Standards Institute (ETSI) also released guidance and standards on IoT as well as specific connected technologies, such as medical devices and intelligent transport systems.

The individual state-focused approach to ensuring cyber-security of all "things" within the IoT ecosystem is a complex task and not reflective of the dynamic threat environment or of the multiple actors that contribute to this space. A hyper-focus on a great-power competition framing of all things technology-focused detracts from the nuances of governing cyber-security risks and oversimplifies possible solutions. Additionally, it risks further fragmentation of guidelines and policies, and sidelines attempts at co-operating for global standardization. Identifying common interests between actors through consultations, recommendations and regulations is perhaps a more productive endeavour.

Canada was not included in the AUKUS partnership between Australia, the U.K. and the U.S., but there are other avenues for co-operation on technologies besides nuclear submarines; for example, in QC and AI. Canada should ensure that it does not miss an important opportunity for co-operation with our most trusted partners. Although Budget 2022 emphasized co-operation with NATO and NORAD to address ongoing challenges and collective security, other co-operation remains important to foster, especially in addressing cyber-security challenges. The FVEY (Australia, Canada, New Zealand, the U.K. and the U.S.) partners routinely release joint advisories[5] on a number of cyber-security issues and mitigation strategies or recommendations. In 2019, the FVEY partners released a communiqué outlining guidance on the security of IoT through the U.K.'s Home Secretary. Perhaps going further and creating a collaborative FVEY working group to address IoT cyber-security risks, including best practices, and exploring regulations and standards would put some of these agreements and guidance into practice.

[5] In collaboration with the Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC), United Kingdom's National Cyber Security Centre (NCSC), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and the Federal Bureau of Investigation (FBI).

About the Author

Kristen Csenkey *is a Fellow with CGAI and the 2020 Women in Defence and Security (WiDS) Fellowship recipient. She is a PhD candidate at the Balsillie School of International Affairs in Waterloo.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.