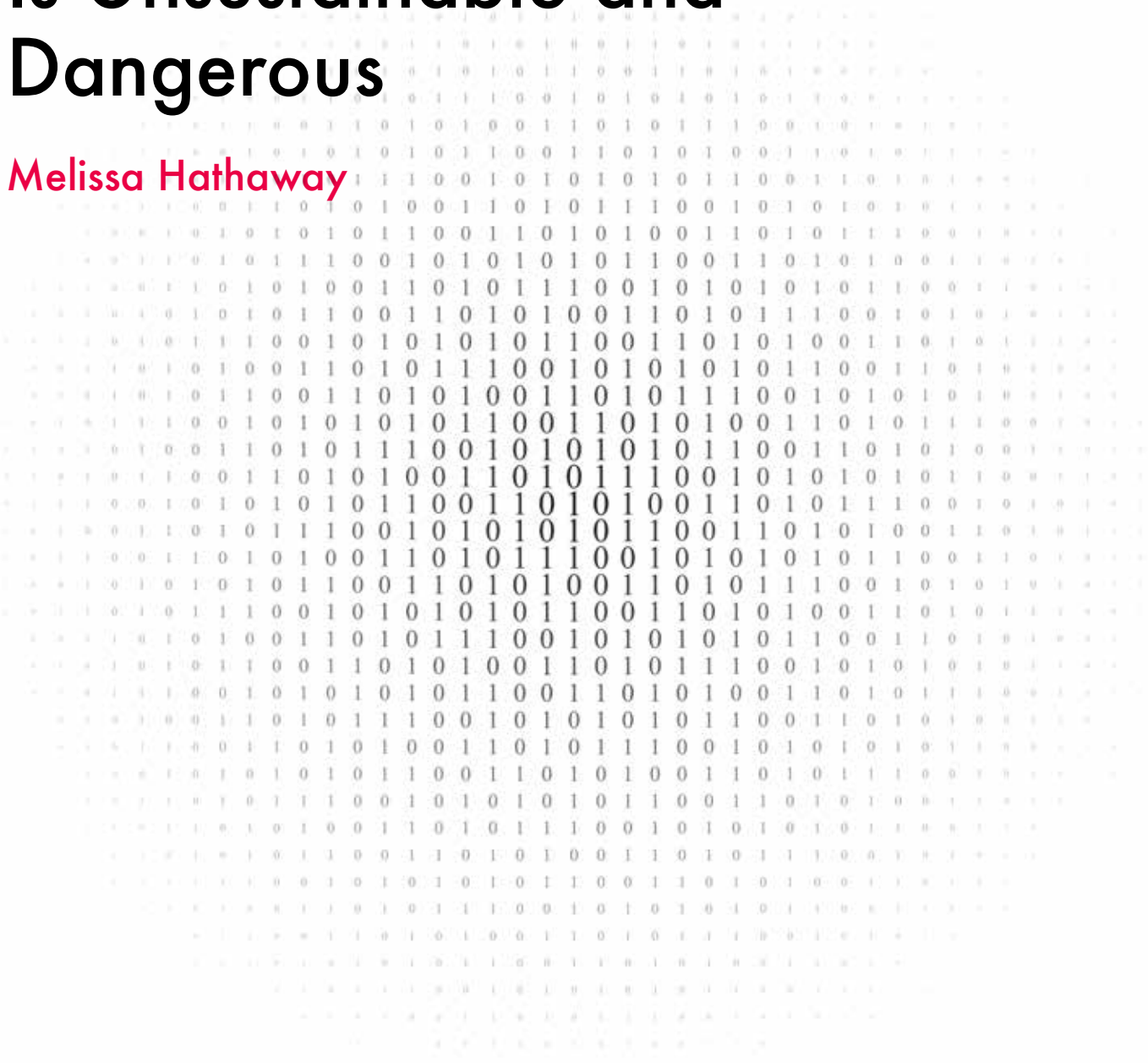
Centre for International
Governance Innovation

CIGI Papers No. 219 — June 2019

Patching Our Digital Future Is Unsustainable and Dangerous

Melissa Hathaway



Centre for International
Governance Innovation

CIGI Papers No. 219 — June 2019

Patching Our Digital Future Is Unsustainable and Dangerous

Melissa Hathaway

CIGI Masthead

Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the Global Economy Program Robert Fay
Director of the International Law Research Program Oonagh Fitzgerald
Director of the Global Security & Politics Program Fen Osler Hampson
Director of Human Resources Laura Kacur
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Senior Publications Editor Nicole Langlois
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz
Graphic Designer Melodie Wakefield

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

Communications

For media enquiries, please contact communications@cigionline.org.

@cigionline

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

Centre for International Governance Innovation and CIGI are registered trademarks.

Centre for International Governance Innovation

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

Table of Contents

About the Author

Melissa Hathaway joined the Centre for International Governance Innovation's Board of Directors in March 2019. Melissa is president of Hathaway Global Strategies LLC, where she brings a multidisciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. She served in two US presidential administrations, leading the Comprehensive National Cybersecurity Initiative for President George W. Bush and spearheading the Cyberspace Policy Review for President Barack Obama.

Melissa has served on the board of directors for three public companies and three non-profit organizations and is a strategic adviser to a number of public and private companies. She brings a unique combination of policy and technical expertise, as well as boardroom experience, to help others better understand the intersection of government policy, developing technological and industry trends, and the economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cyber security matters affecting companies and countries.

Melissa has a B.A. degree from American University in Washington, DC, and is a graduate of the US Armed Forces Staff College, with a special certificate in information operations.

Acronyms and Abbreviations

CBMS	confidence-building measures
CII	critical information infrastructures
COTS	commercial-off-the-shelf
GGE	Group of Governmental Experts
ICS	industrial control systems
ICT	information and communications technology
IoT	Internet of Things
IT	information technology
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Cooperation in Europe

Executive Summary

In recent years, the world has witnessed an alarming number of high-profile cyber incidents, harmful information and communications technology (ICT) practices, and internationally wrongful acts through the misuse of ICTs. Over the last 30 years, a unique and strategic vulnerability has been brought to society — by allowing poorly coded or engineered, commercial-off-the-shelf (COTS) products to permeate and power every aspect of our connected society. These products and services are prepackaged with exploitable weaknesses and have become the soft underbelly of government systems, critical infrastructures and services, as well as business and household operations. The resulting global cyber insecurity poses an increasing risk to public health, safety and prosperity. It is critical to become much more strategic about how new digital technologies are designed and deployed, and hold manufacturers of these technologies accountable for the digital security and safety of their products. The technology industry has fielded vulnerable products quickly — now, it is crucial to work together to reduce the risks created and heal our digital environment as fast as society can.

Introduction

Innovative technologies of the twentieth century have profoundly transformed society and the economy. The first electronic message was sent nearly 50 years ago on October 29, 1969 (over the Advanced Research Projects Agency Network, or ARPANET, the network that became the basis for the internet), but the internet did not become an engine of commerce until 1985 with the introduction of the .com top-level domain (Hathaway 2012). E-commerce was made easier with the launch of the World Wide Web in 1990 and was further accelerated by affordable computing power embedded with functionality and a wide range of applications in the palm of our hands (mobile phones). Nations and corporations alike have since embraced, adopted and embedded ICT into their networked environments and infrastructures, and realized phenomenal business and economic growth through improved services, increased productivity and decreased costs. Today, the digital economy represents about 20 percent of global GDP (Wladawsky-Berger 2017; Huawei and Oxford Economics 2017) and, by 2020, at least 30 billion Internet of Things (IoT) devices will hyper-connect our countries' infrastructures and businesses and generate US$8 trillion in global revenue (Cleo 2018).

Yet this digital transformation — underpinned by affordable communications and cheap devices — has introduced new risks that cannot be ignored. The decision to embrace and embed often poorly coded or engineered, commercial-off-the-shelf technologies into every part of our connected society — from government systems to critical infrastructures and services to businesses and households — is not without consequences. The providers of these technologies — the ICT vendors — are incentivized to be first to market with their products, and the marketplace has simply accepted the vendors' promise that they will fix or "patch" the flaws in their products later. For example, Microsoft formalized this regular patching process in October 2003 — it has become known as "patch Tuesday." Other vendors patch on a less frequent basis with little transparency on the known vulnerabilities that they have transferred to our digital products and services. Patch Tuesday is inevitably followed by a "vulnerable Wednesday" — where malicious actors, who are now also aware of those newly disclosed vulnerabilities, can exploit unpatched systems and steal sensitive data, knock businesses offline and, in some cases, destroy the information technology (IT) systems that power businesses and essential services. Most organizations are not able to promptly update their systems when patches are released, further heightening our collective vulnerability to cyber harm.

The gold standard for implementing a software patch is 30 days (Proviti 2017). Other organizations may take longer to implement a software update in order to complete proper testing of systems to ensure that other business applications or processes are not negatively impacted. Still others may choose not to update their software for fear of breaking legacy applications within older and most likely end-of-life systems. To put this in perspective, Microsoft's patch Tuesday in April 2019 included 15 software patches to address at least 74 vulnerabilities in its Windows

operating systems and supporting software, including two zero-day bugs (Krebs 2019a). The previous patching update, in March 2019, similarly addressed more than five dozen vulnerabilities in Windows operating systems, Internet Explorer, Edge, Office and Sharepoint (Krebs 2019b). This "field it fast, fix it later" ethos has increased our exposure and is leading to real economic losses. For example, cybercrime is growing at 26 percent per year and is estimated to cost the global economy at least US$2.1 trillion in 2019 — or two percent of global GDP (Symantec 2018). Moreover, IoT attacks have increased by 600 percent between 2016 and 2017, in large part because of the ease to exploit connected devices (ibid.).

The flagrant ease with which these vulnerabilities can be exploited is often lost on both the general public and policy makers. For instance, Shodan — a free and publicly available search engine developed to locate digitally connected devices — can be used to easily find unpatched systems (Hill 2013). The tools needed to exploit known vulnerabilities are also inexpensive and easy to wield. Whether you purchase the book *Hacking for Dummies*, or hire a professional dark-web-market service, the ability to cause harm is no longer solely the purview of nation-states. Distributed denial-of-service attacks can be executed for as little as US$700, while stolen bank credentials can be purchased for the price of a cup of coffee (Barysevich 2017). Unauthorized access to accounts on Instagram, Twitter, Snapchat or other social media platforms costs just over US$100 (McCamy 2018; Dell SecureWorks 2016). If you are interested in compromising a corporation, it may only cost US$500 to hijack a corporate mailbox. In 2017, compromises of business email resulted in over US$650 million in losses in the United States alone (Federal Bureau of Investigation 2017).

The Cost of Global Cyber Insecurity

The economic and societal consequences of this widespread vulnerability are becoming increasingly acute. The world bears witness to a growing number of high-profile cyber incidents resulting in risks to public health and safety, global transportation and commerce and key industrial manufacturers. For example, in May 2017, a particularly simple strain of ransomware called WannaCry targeted flaws in Microsoft Windows operating systems, affecting millions of computers in 150 countries across every business sector. This global attack halted manufacturing operations, transportation systems and telecommunications systems. According to the National Audit Office in the United Kingdom, WannaCry affected at least 81 of the 236 National Health Service trusts — rendering medical equipment inoperable and significantly affecting public health and safety (National Audit Office 2017).

Six weeks later, in June 2017, a destructive malicious software called NotPetya swept the world, destroying the capital assets of hundreds of companies in minutes. Business operations halted in many companies, including Maersk (shipping), Merck (pharmaceuticals), Mondelez (confections) and DLA-Piper (legal services). Shipping giant A.P. Moller-Maersk was one of the companies most affected by this attack. It is responsible for the management of 76 port facilities worldwide and roughly 20 percent of the world's container shipping capacity (Reuters 2017). It was figuratively and literally dead in the water after NotPetya spread across its entire global network. Within minutes, the virus encrypted and wiped the company's information technology systems globally, including 4,000 servers, 45,000 computers and 2,500 applications across 600 locations in 130 countries. Maersk's systems were offline for more than 150 hours (Maersk books an average revenue of US$2.9 million per hour) and the company reported first-quarter losses in the order of US$435 million to replace the IT systems that powered its digital business (A.P. Moller-Maersk 2017). Ultimately, it lost 10 percent of its market share to China Ocean Shipping Company. Maersk's shareholder value depreciated by 30 percent within nine months of the incident and depreciated more than 50 percent 18 months post incident.[1] In addition, Denmark's GDP was also negatively impacted as Maersk contributes at least seven percent of the country's GDP. The second- and third-order consequences to global shipping and the global economy have not been quantified (Greenberg 2018).

1 Maersk share price was at a high of around 14,000 Danish krones just before the NotPetya attack. Six months after the event, its share price had dropped to around 10,000 Danish krones. One year post incident, the share price dropped further to 8,000 Danish krones.

Now, Maersk executives talk about the importance of recovery operations since it took a whole-of-company effort to get the business back online (Palmer 2019). However, Maersk was aware of its digital vulnerabilities and the need for cyber security improvements prior to NotPetya's release (A.P. Moller-Maersk 2016). Maersk may have weathered the storm better if it had implemented standard security procedures, such as regular updates to its software and operating systems and development of network segmentation.

The economic damages caused by NotPetya and WannaCry can be measured in the hundreds of billions of dollars. Yet, there are fears that global businesses are still unprepared for a global outbreak of another ransomware or destructive attack. In the first quarter of 2019, the new LockerGoga ransomware exploited unpatched Microsoft systems, knocking offline French engineering consultancy Altran Technologies, Japanese optical products manufacturer HOYA Corporation and American chemical companies Hexion and Momentive (Franceschi-Bicchierai 2019), as well as Norwegian Norsk Hydro — one of the world's largest aluminum manufacturers (Ashford 2019).

As more companies connect and instrument their businesses to the IoT, their exposure to product vulnerabilities and exploitation thereof will also increase — putting their business operations at risk. Software and hardware design vulnerabilities should be addressed in those products' design and development phases prior to debuting in active, high-stakes industrial operations. Critical infrastructure such as energy grids, manufacturing centres and petrochemical plants are increasingly coming under attack from malware designed to infiltrate industrial control systems (ICS) in order to disable, disrupt or seize control of the hardware. For example, the Triton malware was designed to sabotage critical operational technology in ICS, map the industrial network, and allow attackers to remotely control systems (Sobczak 2019). The first instance of its use was discovered in a Middle Eastern petrochemical facility in 2017. Although Triton was foiled by a flaw in its own design, it could have been used to override the shutdown procedures, which normally prevent disasters such as explosions or leakage of toxic chemicals (Giles 2019; Vijayan 2017; Jackson Higgins 2018). The malware exploited a vulnerability in Schneider Electric's Triconex safety instrumented system. The system is deployed in 73 countries across numerous sectors including refining, petrochemicals, chemicals and specialty chemicals, power generation and pharmaceuticals (Desruisseaux 2018). As industrial manufacturers embark on their digital transformation, automating their processes and embedding IoTs in their business lines, their risk of digital disruption and asset destruction also increases. The use of sophisticated malicious software to target these systems is on the rise — and is alarming.

Interstate Behaviour in Cyberspace: Hostility on the Rise

The danger of interstate cyber hostility is also imminent. According to the 2019 US National Intelligence Strategy, "cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices" (Office of the Director of National Intelligence 2019). Cyber insecurity is taxing our economy and destabilizing our security. Each vulnerability is only a keystroke away from being exploited with weapons and services that are easily accessible and affordable online. Individuals, organizations and nation-states are increasingly taking advantage of these vulnerabilities to illegally copy intellectual property to advance economic interests; seize personal identifiable information to monetize in the dark market and pilfer universities' research to advance sovereign interests; steal money or cryptocurrency to skirt the impacts of sanctions; and seed distrust among political parties, leaders and countries. As a testament to the growing anxiety around interstate cyber hostilities, in 2018, the United States and the United Kingdom took the unprecedented step of jointly calling out another state, warning that Russia had been infiltrating energy and transportation infrastructure, nuclear facilities and critically important private sector firms (US Department of Homeland Security 2018).

Numerous multilateral institutions have been promoting the responsible use of technology and advocating for normative or "responsible"

behaviour among nations. Ensuring international agreement on what is proper and what is not proper behaviour in cyberspace is a priority for almost every country seeking to create stability and safety in cyberspace (Finnemore and Hollis 2016; Henriksen 2019). The first set of discussions in this regard was proposed by Russia in 1998. The UN Secretary General established a Group of Governmental Experts (GGE) to study the "developments in the field of information and telecommunications in the context of international security."[2] Since 2004, five GGEs have continued to study the threats posed by the misuse of ICTs in the context of international security and how these threats should be addressed. Three of these groups have agreed on substantive reports with conclusions and recommendations.[3]

In July 2015, member countries of the UN GGE endorsed and adopted a new set of voluntary, non-binding norms of responsible state behaviour in cyberspace. One of the most important norms agreed to by the group stated that "a State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (UN General Assembly 2015, para. 13[f]). However, as demonstrated by the WannaCry incident (attributed to North Korea), the NotPetya destructive attack (attributed to Russia) and other similar attacks against companies and countries, states' actions often do not match their professed ideals and norms of conduct are routinely ignored (Hathaway 2017, 2). Intentional damage of other nations' infrastructure is becoming tacitly accepted as the normal state of affairs.

In September 2017, UN Secretary General António Guterres stated that "cyber war is becoming less and less a hidden reality — and more and more able to disrupt relations among States and destroy some of the structures and systems of modern life" (UN Secretary General 2017). He acknowledged that traditional forms of regulations do not apply, signalling a need for strategic thinking, ethical reflection and thoughtful regulation (ibid.). At the December 2018 UN General Assembly plenary meeting, two processes were launched to discuss the issue of security in the ICT environment for the period 2019–2021. Resolution 73/27, proposed by the Russian delegation, established an Open-Ended Working Group, which will be comprised of the entire UN membership (UN General Assembly 2018a; 2018b). It will further the development of norms and principles for responsible state behaviour in cyberspace and will look for meaningful ways to implement them. The group will deliver a final report at the seventy-fifth session of the UN General Assembly in September 2020. Another resolution, proposed by the United States, established a new GGE on "advancing responsible state behavior in cyberspace in the context of international security" (UN General Assembly 2019). This group will continue to study possible cooperative measures to address information security threats.

Other international organizations have also been promoting the responsible use of technology in order to build trust and confidence in the use of ICTs and minimize cyber harm. The 57 member states of the Organization for Security and Cooperation in Europe (OSCE), for example, have adopted 16 confidence-building measures (CBMs) to reduce the risks of conflict stemming from the misuse of ICTs and to increase cooperation among states to protect their critical infrastructures. The OSCE believes that increasing direct communication among states will defuse conflicts and prevent unintentional escalation. The language in the document is that of a non-legally binding agreement, but it is a step toward advancing international cooperation in cyberspace in order to promote best practices and address vulnerabilities affecting our economy. Other multilateral institutions have adopted these CBMs, including the Organization of American States and the Association of Southeast Asian Nations.

Yet, in parallel to these confidence-building and norm-setting efforts, countries are also developing their own offensive cyber capabilities to deter or possibly respond to cyber attacks. The problem is that they are fighting fire with fire. For example, in 2016, at the North Atlantic Treaty Organization (NATO) Warsaw Summit, the alliance declared cyberspace as the fifth domain of warfare. Since that time, seven members have pledged their offensive cyber weapons to the alliance and stand ready to employ the full force of their arsenal should one member fall

2 See www.un.org/disarmament/ict-security/.

3 UN GGEs substantive reports include: 2009/2010 – A/65/201; 2012/2013 – A/68/98*; 2014/2015 – A/70/174. See www.un.org/disarmament/ict-security/.

victim to a particularly grievous cyber attack.[4] From now on, NATO will integrate the sovereign effects from the nations that are capable and willing to provide them (Freedberg 2018).

The Role of Governance in Reducing Cyber Risk

The digital environment continues to underpin our homes, businesses and countries with products and services that are pre-packaged with exploitable weaknesses. The high-profile cyber security incidents of recent years are symptomatic of the attitude that continues to dominate the development and commercialization of digital technology, in which companies strive to release products as quickly as possible and worry about security flaws after they have already been deployed. Ultimately, the paradigm of "field it fast, fix it later," which continues to hold sway in the technology industry, must be overcome. If we are to achieve a stronger level of security or at least significantly reduce cyber risk in the digital age, governments will need to step in and hold digital service providers and the manufacturers of ICT technology accountable for ensuring their products maintain adequate cyber safety standards.

As the scale of the threat has become more apparent, governments around the world have turned to developing frameworks for understanding the nature of their digital dependency, cyber security strategies for fending off these threats and policies to establish standards of safe behaviour.

For example, in the United States, the Department of Commerce is launching an initiative to improve transparency around software components. The so-called Software Bill of Materials intends to drive a disclosure process for all software and IoT vendors to share the details on the underlying components, libraries and dependencies of their software with their customers. According to Allan Friedman, director of cyber security for the National Telecommunications and Information Administration, "this transparency can catalyze a more efficient market for security by allowing vendors to signal quality and giving enterprise customers key knowledge — you can't defend what you don't know about" (Friedman quoted in Epper Hoffman 2018). It would also give enterprises more insight into the risks to their digital businesses (i.e., patch Tuesday).

If this initiative does not catalyze industry to take more responsibility for the inherent flaws in their products, the state of California has taken an even more proactive approach. In anticipation of the unfolding IoT vulnerabilities, California passed a connected devices law, which lays out the security features that must be included in all digitally connected devices.[5] The law will go into effect on January 1, 2020. It requires vendors that intend to sell connected devices (i.e., IoT) in California to implement enhanced security measures for all those products. It broadly defines devices as any device that connects *directly or indirectly* to the internet and has an Internet Protocol or Bluetooth address. These security measures include device attestation, code signing and a security audit for firmware in low-level components.

In Europe, the General Data Protection Regulation (Council of the European Union 2016), which entered into force in May 2018, aims to hold companies accountable for the digital security of personal information. The Network and Information Security Directive stipulates minimum standards of care for the cyber security of critical infrastructure, including energy, transport, banking, finance, health, water and digital infrastructures such as online marketplaces (for example, eBay and Amazon), search engines (for example, Google) and clouds. Companies that suffer a significant breach or service outage must notify the relevant national authority within 48 hours and include the following data points: duration of incident; number of affected parties (for example, customers, vendors, and so on); geographic spread; extent of disruption of service; and impact on economic (calculated in GDP terms) and societal activities.[6]

Similarly, China passed a national cyber security law that went into effect in June 2017. It contains 79 different articles detailing data

4 The seven NATO members that have pledged their offensive cyber weapons to the alliance are Estonia, Denmark, France, Germany, Netherlands, United Kingdom and the United States.

5 See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

6 See https://eur-lex.europa.eu/eli/dir/2016/1148/oj and www.enisa.europa.eu/topics/nis-directive.

protection requirements and cross-border data flow guidelines, as well as specific guidelines for "critical information infrastructures" (CII). This includes information services and the law establishes a broad definition of CII as a service that may cause serious damage to national security, the national economy and public interest if destroyed, if functionality is lost or if data is leaked (Creemers, Triolo andWebster 2018).

The common thread between all these policies is that destructive and disruptive cyber activities require urgent attention and action. National cyber security strategies, no matter how comprehensive, will fail unless clear lines of accountability are drawn, delineating security obligations among relevant parties. Presently, the delegation of duties between government and the private sector remains unclear in many areas, such as the protection of critical infrastructure. This ambiguity makes it particularly difficult to hold organizations responsible for lax security standards. Comprehensive, methodical assessments of cyber risk at the national level will be required to correctly identify the greatest areas of vulnerability and address the gaps in current defensive strategies. Policy makers need to ascertain what risks they are willing to bear and what would be considered intolerable. Risk reduction activities also require the allocation of dedicated and appropriate resources, both human and financial, for their implementation. Only with a concerted and coordinated effort across national stakeholders will it be possible to significantly reduce cyber risk and move forward to ensure the future safety and security of a nation.

All governments are operating under resource constraints and will need to engage in sincere, honest reflections in order to set digital security priorities. Many current policy approaches cast a wide net in terms of which systems are deemed critical to national and economic security. However, by focusing their attention too broadly, countries risk devoting insufficient attention and resources to those few indispensable infrastructures, services, companies and assets upon which everything else depends. The fact of the matter is that some are more important than others. The provision of energy and telecommunications, for example, is essential to the economic health and national security at the most fundamental level, as nearly all other systems would cease to function without them. Certain companies, which comprise a large proportion of the total economy of a country, may also warrant special attention. For instance, A.P. Moller-Maersk contributes a large share of Denmark's GDP, such that when the company fell victim to NotPetya in 2017, the Danish economy suffered significant collateral damage. The United States and Germany have proceeded by identifying companies contributing more than two percent of their national GDP and forging better information-sharing arrangements with them to ensure cyber security concerns are given due consideration in corporate protective measures (Hathaway 2018, 9).

Despite a nearly universal agreement about the importance of shielding critical services and assets from digital harm, governments have thus far had difficulty in accurately assessing where the greatest vulnerabilities lie, and therefore knowing exactly what warrants their immediate attention or is the highest priority. For example, the city of Atlanta — one of the top 100 resilient cities globally — was knocked offline in March 2018 by the SamSam ransomware (Schwartz 2018). Its January 2019 audit showed that the city had known gaps in its security that had not been addressed. Less than six months later, another critical asset in the United States — the port of San Diego — suffered a ransomware attack that used the same variant of malware as the one in Atlanta. SamSam affected IT systems and disrupted public services (Kan 2018). In the Netherlands, despite efforts by the Dutch government to bolster the cyber security of its critical infrastructures and services, officials were caught off guard when the port of Rotterdam (the largest in Europe) fell victim to the NotPetya malware in 2017. Upon further review, Dutch officials discovered that they had not classified ports as critical infrastructure under their infrastructure protection policies (Hathaway 2018). Many critical assets of great importance to economic vitality and national security have been overlooked by current cyber security strategies, necessitating more rigorous countrywide assessments.

Time to Get Strategic

As things currently stand, countries at the cutting edge of the technological frontier are moving forward with the development and deployment

of IoT and other innovative technologies at a breakneck pace. First-mover advantages are perceived to be so great that most relevant actors have not stopped to consider the potentially destabilizing effects of these technologies for fear of falling behind their economic and geopolitical rivals. Yet, by attaining an advantage in this "technological arms race," countries are rendering themselves more dependent on technologies that are increasingly complex and opaque — and thus vulnerable — leading to a higher risk of accidents and unanticipated negative effects. As a recent report from the Center for a New American Security put it, "superiority is not synonymous with security" (Danzig 2018, 7). In the long run, it will be those nations that have given pause to consider the possibilities for adversarial use of the technologies in question that will be best placed to reap rewards in terms of wealth and influence.

Increased automation, interconnectedness and reliance on the internet require that we embrace a new form of cooperation, in which vulnerabilities are reported to the owner of the information system, allowing the organization at stake the opportunity to diagnose and remedy the vulnerability in question before detailed vulnerability information is disclosed to third parties or the public. This is called responsible disclosure. Ideally, vulnerabilities are largely prevented through a design process that gives security higher priority. So far, the ICT industry has followed a different path and many vulnerabilities are repaired only after the product has been embedded in an operational environment and supporting business-critical systems (Internet Engineering Task Force 2002).

The United States maintains a National Vulnerability Database; 78 organizations in 14 countries use the data. Vulnerabilities reported to the Department of Homeland Security's Cyber and Infrastructure Security Agency by way of the US Computer and Emergency Readiness Team are disclosed to the public within 45 days of the initial reporting, regardless of the existence or availability of patches or workarounds from affected vendors. China has a similar system, but it operates twice as fast as the American process, averaging just 13 days after public disclosure. China proactively scours the web and other sources of information, looking for vulnerability information, whereas the United States waits for reports from vendors to be processed through the Common Vulnerabilities and Exposures database (Waterman 2017).

The trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences. From a government point of view, disclosing a vulnerability can mean that intelligence agencies forego an opportunity to collect crucial intelligence that could thwart a terrorist attack, stop the theft of a nation's intellectual property or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks (The White House 2014). But when a corporation decides not to disclose critical unfixed vulnerabilities in its software, should that be considered okay? What about when the database of all known vulnerabilities is illegally copied by malicious actors? Is there an obligation to disclose the loss and begin addressing the risk that the corporation has now transferred to society? In 2013, hackers obtained unauthorized access to a Microsoft database that contained descriptions of critical and unfixed vulnerabilities in its software, including the Windows operating system (Menn 2017). In August 2016, government tools that were largely focused on exploiting these Microsoft vulnerabilities began to be publicly released — presenting a real risk to global corporations and the global economy. Some of these tools (or weapons) were ultimately behind the WannaCry and NotPetya attacks in 2017 (Patel 2017; Hay Newman 2017; Schneier 2017).

In February 2017, Microsoft launched a campaign to deflect attention from its flawed products and put the responsibility for the exploitation of those vulnerabilities back onto nations. It launched its "Digital Geneva Convention" campaign, stating that governments should commit to "protecting civilians from nation-state attacks in times of peace." The document asserts that "just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross…protection against nation-state cyber attacks requires the active assistance of technology companies." Microsoft affirmed that the tech sector plays a unique role as the internet's first responders, and the technology companies, therefore, should commit themselves to collective action that will make the internet a safer place, affirming a role as a neutral "digital Switzerland" that assists customers everywhere and retains the world's trust (Smith 2017). However, it is too bad that the company chose to pursue a convention

about normative state behaviour vice fixing its own flawed products. Microsoft has gone on to advocate for a "Cybersecurity Tech Accord," launched in 2018, that promises to defend and advance the benefits of ICTs to society. It assumes that technology companies are the rightful heirs that create and operate online technologies. Finally, Microsoft's efforts were highlighted again in the "Paris Call for Trust and Security" that was announced at the opening of the Internet Governance Forum in November 2018. It was supported by governments and private sector organizations around the world. But are we to believe the charlatan who quietly hides their negligence and shifts responsibility to another party? Society needs responsible, ethical and serious corporate leaders who are dedicated to delivering a secure and resilient digital future for all (Tech Accord 2019).

We must become much more strategic in how new digital technologies are created and deployed. Over the last 30 years, we have created a unique and strategic vulnerability to society — an inherently insecure internet supported by poorly engineered products. It is an existential threat to our economy and our sovereign security. To address this immediate threat, an emergency counter-measures board and mitigation process should be initiated that is global and convenes the best talent, regardless of nationality. The industry has fielded us vulnerable products fast — now, we must work together to reduce the risks and heal our digital environment as quickly as society can.

Our governments should require: a new vulnerability disclosure process (and operational requirements); a duty to warn of imminent danger, such as in the case of an emerging attack; and a duty to assist in the case of cyber emergencies (Hathaway and Savage 2012). ICT purveyors of products should be required to implement a new communications and warning system for urgent patches, adding "emergency" to their repertoire of categories (emergency, critical, important, moderate and low).

Consumer protection agencies must also engage. We have been conditioned to marketplace recalls related to food, medicine, automobiles and even children's toys — IT products are not recalled, even when it is known that they can cause serious harm to society. The consumer protection agencies can drive accountability by eliminating or significantly reducing after-market repairs (patch Tuesday) to a market that drives accountability through product recalls. Vendors should have to deliver well-engineered products and services and present the buyer with a list of the underlying components, libraries and dependencies — a "software bill of materials" — to drive transparency and accountability. This process could also inform the emerging revisions of ISO/IEC 29147:2014, Information technology — Security technology — Vulnerability disclosure.[7]

Finally, the UN General Assembly has recognized the importance of reducing the ICT threat to society by launching two new fora to deliberate on normative state behaviours and to look for meaningful cooperative measures to address information security threats. These efforts are essential to develop pathways for direct communications among states and to help prevent unintentional escalation in cyberspace.

The world has witnessed an alarming number of harmful ICT practices and internationally wrongful acts through the misuse of ICTs in recent years. There has been a large, perhaps unwarranted, degree of faith in novel technologies. We tend to trust that technology will always work as intended — and *only* as intended — often failing to give much thought to how the technologies that are created to solve our problems could be turned to nefarious ends. The time has come to recognize this overarching problem and subject technological development to greater scrutiny. The downsides of novel technologies should be contemplated along with the benefits they may bring. Only then will we be able to start eradicating the vulnerabilities from the core of our digital future.

7 This international standard ISO/IEC DIS 29147 revision is currently under development.

Works Cited

A.P. Moller-Maersk. 2016. *Annual Report 2016.* http://investor.maersk.com/static-files/a31c7bbc-577a-49df-9214-aef2d649a9f5.

———. 2017. *Annual Report 2017*. http://investor.maersk.com/news-releases/news-release-details/annual-report-2017.

Ashford, Warwick. 2019. "Norsk Hydro urges caution as it counts cost of cyber attack." *Computer Weekly,* May 3. www.computerweekly.com/news/252462778/Norsk-Hydro-urges-caution-as-it-counts-cost-of-cyber-attack.

Barysevich, Andrei. 2017. "Dissecting the Costs of Cybercriminal Operations." *Recorded Future* (blog), November 2. www.recordedfuture.com/cyber-operations-cost/.

Cleo. 2018. "10 Mind-Boggling Figures that Describe the Internet of Things (IoT)." Cleo, June 4. www.cleo.com/blog/internet-of-things-by-the-numbers.

Council of the European Union. 2016. "General Data Protection Regulation (EU 5419/16)." April 6. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Creemers, Rogier, Paul Triolo and Graham Webster. 2018. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *New America*, June 29.

Danzig, Richard. 2018. "Technology Roulette: Managing Loss of Control as Militaries Pursue Technological Superiority." Center for a New American Security, May 30. www.cnas.org/publications/reports/technology-roulette.

Dell SecureWorks. 2016. "Underground Hacker Markets: Annual Report." April. http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf.

Desruisseaux, Daniel. 2018. "Cyber-Nationalism in Cybersecurity Standards." *Schneider Electric Blog,* April 16. https://blog.schneider-electric.com/cyber-security/2018/04/16/cyber-nationalism-in-cybersecurity-standards/.

Epper Hoffman, Karen. 2018. "Assembling an Ingredients List for Software." GCN, August 24. https://gcn.com/articles/2018/08/24/software-bill-of-materials.aspx.

Federal Bureau of Investigation. 2017. "Internet Crime Report." https://pdf.ic3.gov/2017_IC3Report.pdf.

Finnemore, Martha and Duncan Hollis. 2016. "Constructing Norms for Global Cybersecurity." *The American Journal of International Law* 110 (3): 425–79.

Franceschi-Bicchierai, Lorenzo. 2019. "Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers.'" Mother Board, March 23. https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers.

Freedberg, Sydney. 2018. "NATO To 'Integrate' Offensive Cyber By Members." Breaking Defense, November 16. https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/.

Giles, Martin. 2019. "Triton is the World's Most Murderous Malware, and it's Spreading." *MIT Technology Review*. March 5. www.technologyreview.com.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired,* August 22. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hathaway, Melissa. 2012. "Falling Prey to Cybercrime: Implications for Business and the Economy." In *Securing Cyberspace: A New Domain for National Security*, edited by Nicholas Burns and Jonathon Price, 145–57. Aspen, CO: The Aspen Institute.

———. 2017. *Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice*. CIGI Paper No. 127. Waterloo, ON: CIGI. www.cigionline.org/publications/getting-beyond-norms-when-violating-agreement-becomes-customary-practice.

———. 2018. "Managing National Cyber Risk." Organization of American States. White Paper Series, Issue 2. www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

Hathaway, Melissa and John E. Savage. 2012. "Duties for Internet Service Providers." Paper presented at Cyber Dialogue 2012. Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, March.

Hay Newman, Lyli. 2017. "The biggest cybersecurity disaster of 2017 so far." *WIRED,* July 1. www.wired.com/story/2017-biggest-hacks-so-far/.

Henriksen, Anders. 2019. "The end of the road for the UN GGE process: The future regulation of cyberspace." *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyy009.

Hill, Kashmir. 2013. "The Crazy Things a Savvy Shodan Searcher Can Find Exposed on the Internet." *Forbes*, September 5. www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/#510502793c7e.

Huawei and Oxford Economics. 2017. "Digital Spillover: Measuring the true impact of the digital economy." September 5. www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf.

Internet Engineering Task Force. 2002. "Responsible Vulnerability Disclosure Process." February. https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00.

Jackson Higgins, Kelly. 2018. "Schneider Electric: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT." Dark Reading, January 18. www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845.

Kan, Michael. 2018. "Ransomware Strikes the Port of San Diego, Disabling IT Systems." *PC Magazine*, September 28. www.pcmag.com/news/364081/ransomware-strikes-the-port-of-san-diego-disabling-it-syste.

Krebs, Brian. 2019a. "Patch Tuesday Laydown, April 2019." *Krebs on Security* (blog), April 9. https://krebsonsecurity.com/2019/04/patch-tuesday-lowdown-april-2019-edition/.

———. 2019b. "Patch Tuesday Laydown, March 2019." *Krebs on Security* (blog), March 19. https://krebsonsecurity.com/2019/03/patch-tuesday-march-2019-edition/.

McCamy, Laura. 2018. "7 Things You Can Hire a Hacker to do, and How Much it will (Generally) Cost." *Business Insider*, November 27. www.businessinsider.com/things-hire-hacker-to-do-how-much-it-costs-2018-11.

Menn, Joseph. 2017. "Exclusive: Microsoft responded quietly after detecting secret database hack in 2013." Reuters, October 17. www.reuters.com/article/us-microsoft-cyber-insight/exclusive-microsoft-responded-quietly-after-detecting-secret-database-hack-in-2013-idUSKBN1CM0D0.

National Audit Office. 2017. "Investigation: WannaCry cyber attack and the NHS." October 27. www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

Office of the Director of National Intelligence. 2019. "National Intelligence Strategy of the United States of America." www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

Palmer, Danny. 2019. "Ransomware: The Key Lesson Maersk Learned from Battling the NotPetya Attack." ZD Net, April 29.

Patel, Andy. 2017. "Petya: 'I Want To Believe.'" *F-Secure* (blog), June 29. https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/.

Proviti. 2017. "How Long Does It Take to Implement a Patch?" Board Perspectives: Risk Oversight. Issue 97. www.protiviti.com/US-en/insights/bpro97.

Reuters. 2017. "Global Shipping Giant Maersk is Reeling from the Ransomware Fallout." *Fortune*, June 29. http://fortune.com/2017/06/29/petya-goldeneye-maersk-ransomware-effects/.

Schneier, Bruce. 2017. "Who Are the Shadow Brokers?" The Atlantic, May 23. www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Schwartz, Mathew. 2018. "Atlanta's Ransomware Cleanup Costs Hit $2.6 Million." GovInfoSecurity, April 24. www.govinfosecurity.com.

Smith, Brad. 2017. "The Need for a Digital Geneva Convention." *Microsoft Blog*, February 14. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Sobczak, Blake. 2019. "The inside story of the world's most dangerous malware." E&E News, March 7. www.eenews.net/stories/1060123327.

Symantec. 2018. *Internet Security Threat Report*. Volume 23, March. www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

Tech Accord. 2019. "Reducing tensions in cyberspace by promoting cooperation. Cybersecurity Tech Accord publishes a set of recommendations on confidence-building measures in cyberspace." April 4. https://cybertechaccord.org/reducing-tensions-in-cyberspace-by-promoting-cooperation-cybersecurity-tech-accord-publishes-a-set-of-recommendations-on-confidence-building-measures-in-cyberspace/.

The White House. 2014. "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities." April 28. https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

UN General Assembly. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." July 22. https://undocs.org/A/70/174.

———. 2018a. "General Assembly Adopts 67 Disarmament Drafts, Calling for Greater Collective Action to Reduce Arsenals, Improve Trust amid Rising Global Tensions." Press release, December 5. www.un.org/press/en/2018/ga12099.doc.htm.

———. 2018b. "Resolution adopted by the General Assembly on 5 December 2018." A/RES/73/27. December 11. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

———. 2019. "Resolution adopted by the General Assembly on 22 December 2018." A/RES/73/266. January 2. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266.

UN Secretary General. 2017. "Secretary General's Address to the General Assembly." September 19.

US Department of Homeland Security. 2018. "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." March 15. www.us-cert.gov/ncas/alerts/TA18-074A.

Vijayan, Jai. 2017. "TRITON Attacker Disrupts ICS Operations, While Botching Attempt to Cause Physical Damage." Dark Reading, December 14. www.darkreading.com/attacks-breaches/triton-attacker-disrupts-ics-operations-while-botching-attempt-to-cause-physical-damage-/d/d-id/1330650.

Waterman, Shaun. 2017. "China's vulnerability disclosure system twice as fast as U.S. version." CyberScoop, October 23. www.cyberscoop.com/china-vulnerability-reporting-nvd-recorded-future/.

Wladawsky-Berger, Irving. 2017. "GDP Doesn't Work In A Digital Economy." *The Wall Street Journal,* November 3. https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy/.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and have received support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques internationales, et le droit international. Nous comptons sur la collaboration de nombreux partenaires stratégiques et avons reçu le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Centre for International
Governance Innovation

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

@cigionline