Renewing our Democratic Alliance

Securing Cyberspace in an Age of Disruption

A Glimpse at the Rising Threatscape

Prepared by Aaron Shull[1] & Kailee Hilt[2]

***Setting the Context**:*

Imagine being a healthcare worker at one of the busiest hospitals in the country. You have been on the frontlines of fighting this pandemic. It has been a distressing year. You have been pushed beyond your limits and are facing heightened levels of stress and anxiety. While making your way through the hospital corridors there is an unsettling sight plaguing the premises. Every surrounding computer screen is pitch-black.

A massive cyber-attack has just transpired and has wreaked havoc on the hospital's computer network. The clock is beginning to tick down ominously, like a timer connected to a bomb in an action movie. Systems are completely crippled, the impact sprawling and dangerous, forcing mass cancellation of routine appointments, obstructing access to patients' records, while hobbling testing and other key treatment services. Hospital personnel are left with no choice but to return to using pens and paper, jeopardizing the delivery of services to those who urgently need them. It will likely be weeks before systems will be fully recovered, putting patients at risk, with each day creating more of a backlog, and aggregating increased pressure on an already exhausted healthcare system.

On May 14th, 2021, cyber criminals targeted the systems of Ireland's Health Service Executive (HSE) as well as many hospital servers, leaving some systems offline for 10 days. It is a trend that has, unfortunately, been seen in many parts of the world since the pandemic started. This particular incident was considered one of the worst cyber-attacks in the country's history. The assailants (thought to be based in Russia) developed the ransomware used in the attack, demanding nearly $20 million in payment, and threatening to sell the stolen data on the dark web. The incident occurred shortly after the paralyzing attack on the Colonial Pipeline in the United States that triggered fuel shortages across the eastern seaboard and saw four states declare states of emergency. It also followed the attack on JBS, the world's largest meat producer.

[1] Aaron Shull is the managing director and general counsel at the Centre for International Governance Innovation.
[2] Kailee Hilt is a research associate at the Centre for International Governance Innovation.

Amid the global gold rush for digital weapons, there is a dramatic escalation in digital malfeasance. Cyberattacks are becoming more common, as hackers are growing significantly in quantity, and technical sophistication. In 2020 alone the global surge in ransomware attacks hit a 102% increase compared to the previous year, with over 28 million Canadians affected by a data breach, and major digital attacks doubling in the US, Europe, Asia, and the Americas.

Attacks have been launched on power grids, solar power firms, water treatment plants, federal and local government agencies, and even police departments' -to name a few. However, the rise of Internet connectivity has ignited a wide spectrum of security vulnerability that spans beyond our critical infrastructure. Foreign interference is undermining the integrity of our democracy. Misinformation is tearing at the seams of social cohesion and weakening trust in institutions. Cyber-espionage is jeopardizing intellectual property and other capabilities that are crucial to our nation's security and prosperity.

Even more worrisome (perhaps) are the efforts that are still in the early stages of development. For instance, there is the use of AI-driven programs, such as "deepfake" technology, that uses machine-learning algorithms that can create convincing impersonations and be used to trick targets into handing over sensitive information. Or quantum computers that can easily break encrypted datasets that organizations have been protecting for decades. Or 5G networks that will ensure that Internet connectivity touches almost every aspect of the economy and modern life.

The nature of these attacks and their sheer scale is game-changing. With cyberspace infiltrating almost every facet of our daily lives, there is blurring in the boundaries between our virtual and physical worlds. With this, the continual stream of data seeping through our connected devices and our (potentially unsecure) networks are building new barriers, widening old gaps, and sowing mistrust like never before. No single government department or agency can address this alone. If we want to be effective in countering modern threats, we must build strategic partnerships, within and outside governments to facilitate ongoing information sharing and consultation, the pooling of resources or expertise, and – if necessary – joint actions.

This scene-setting paper will seek to lay the foundation for a discussion on securing cyberspace in an age of disruption. It will outline some of the challenges that are driving the threat landscape and will discuss tactics for cyber resilience in a world of rising digital tension.

Global Cyber Security Challenges

a) The breakdown of trust between states: A glance at the current international rules structure

We are on the brink of a digital arms race, where our nation-state adversaries and proxies use cyber capabilities as an element of national power and strategic advantage. In this obscure battlefield, "victories are fought with bits instead of bullets, malware instead of militias, and botnets instead of bombs."[3] The rapid development of information technology and the extensive use of the internet has resulted in conflicting views on the application of international law to

[3] Geers et al. 2014. Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. *FireEye.*

cyberspace and cyber operations, making international cooperation both pressing and imperative. However, there is a contentious question about whether existing international legal provisions provide adequate guidance and guarantees for states' relations since state and non-state actors are increasingly pursuing their agendas in the "grey zone" that exists just below the threshold of armed conflict. According to the *Strong, Secure, Engaged Defence Policy*:

> State and non-state actors are increasingly pursuing their agendas using hybrid methods in the "grey zone" that exists just below the threshold of armed conflict. Hybrid methods involve the coordinated application of diplomatic, informational, cyber, military, and economic instruments to achieve strategic or operational objectives. They often rely on the deliberate spread of misinformation to sow confusion and discord in the international community, create ambiguity and maintain deniability. The use of hybrid methods increases the potential for misperception and miscalculation. Hybrid methods are frequently used to undermine the credibility and legitimacy of a national government or international alliance. By staying in the fog of the grey zone, states can influence events in their favour without triggering outright armed conflict. The use of hybrid methods presents challenges in terms of detection, attribution and response for Canada and its allies, including the understanding and application of NATO's Article 5.[4]

Even though there have been significant efforts to advance the conversation surrounding the applicability of pre-cyber era international law to cyber operations, with the leading authority on the subject likely being the Tallinn Manual on the International Law Applicable to Cyber Warfare, several legal scholars continually question the prudence of attempting to apply laws that were designed before computers existed. Why not update the international governance structure to account for contemporary technological realities? This is an especially important conversation to have when many states have remained either silent or vague regarding their position on how existing obligations apply and how these commitments should be improved with respect to principles of due diligence, sovereignty, and countermeasures.

At the outset, there is a distinction that must be made regarding the application of international law to armed conflict and the use of force. This distinction typically breaks down between *jus ad bellum* and *jus in bello*.[5] *Jus in bello* refers to a suite of rules, referred to as international humanitarian law, which is the body of law that governs the way in which warfare is conducted. Put another way, this is the body of rules that govern the conduct of individuals when hostilities are actually occurring. By contrast, *jus ad bellum* is the body of law that can provide either a justification or legal reason for war, or more particularly, the guardrails to prevent international conflict from occurring. This paper will focus only on *jus ad bellum*.

The principal source of *jus ad bellum* remains the United Nations Charter, with the most relevant Articles being Article 2(4) and Article 51. Article 2(4) of the Charter provides that:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

[4] See page 53 of National Defence. 2017. Strong, Secure, Engaged Canada's Defence Policy.
[5] See Carsten Stahn. 2006. 'Jus ad bellum', 'jus in bello' . . . 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force. *European Journal of International Law*, 17 (5), p. 921–943.

While Article 51 provides that:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

To summarize, cyber operations may constitute uses of force pursuant to Article 2(4) of the UN Charter, in turn potentially triggering the right to self-defense in Article 51 – if they reach the threshold of an "armed attack". It is also generally accepted that cyber operations may constitute unlawful interventions in violation of the principle of non-intervention. However, in order to qualify as a use of force or an unlawful intervention, the required degree of intensity is relatively high. Cyber operations have a tendency of constituting very "minimal" uses of force; therefore, not reaching these established intensity thresholds. Essentially this means that cyber operations that do not qualify as a use of force or an unlawful intervention are left in what is construed by some to be an obscure gray area of international law.[6]

There are also no clear rules to govern international economic cyber espionage. Essentially, this lack of rules is leading to a more dangerous and unstable world, since there should be robust international rules prohibiting this conduct, as well as clear, meaningful, multilateral sanctions when impugned conduct is attributable (under international law) to a state. History is dotted with espionage incidents going back centuries, representing a long-term threat to a nation's economy and prosperity. "Such cases of state-sponsored cyber economic espionage [have] targeted companies' business strategies and plans, intellectual property, and expansive research and development projects, eroding their competitive economic advantage in the international marketplace and placing the acquirer an unfair leap ahead on technological developments."[7]

As an example, Chinese actors are the world's most active and persistent perpetrators of economic espionage. General Keith Alexander, former head of the NSA and US Cyber Command, famously noted that China's cyber espionage activities accounted for "the greatest transfer of wealth in history."[8] It is estimated that China is responsible for 50-80% of cross border intellectual property theft worldwide and over 90% of cyber-enabled economic espionage in the US.[9] To put this into further perspective, a 2018 White House report highlights that the cost of trade secret theft from China alone ranges between $180 billion and $540 billion annually for the US.[10]

---

[6] See Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36. *The Yale Journal of International Law*. 421 ("there is considerable momentum among American scholars and policy experts behind the idea that some cyberattacks ought to fall within Article 2(4)'s prohibition of "force" or could constitute an "armed attack," at least insofar as those terms should be interpreted to cover attacks with features and consequences closely resembling conventional military attacks or kinetic force.").

[7] See page 452 of Catherine Lotrionte. 2015. Countering State-Sponsored Cyber Economic Espionage Under International Law. *North Carolina Journal of International Law and Commercial Regulation*, 40(2), 443–538.

[8] See page 2 of Cyber Espionage and the Theft of U.S. Intellectual Property and Technology.

[9] Patrick, Diotte. 2020. The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online. *National Defence and the Canadian Armed Forces.*

[10] See page 3 of How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World. *White House Office of Trade and Manufacturing Policy.*

There are two primary reasons why actors such as China and Russia engage in aggressive cyber economic espionage, while also articulating a norm against it on the international stage,

> First, as a matter of geostrategic interest, China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology. Second, as a technical matter, these types of intrusions rarely get detected, and when they do, they are notoriously difficult to attribute back to a state actor. As a consequence, Russia and China can act in a way that directly contradicts the norm that they are espousing, because there is a relatively low risk of discovery and attribution. It is not in their immediate interests to comply with that norm –the rewards are too high and the risks too low.[11]

Furthermore, there are two parallel rules development initiatives underway at the United Nations. One route, sponsored by the United States, is the Group of Governmental Experts (GGE) mandated to study how international law applies to state action in cyberspace and identifies ways to promote compliance with existing cyber norms.

The GGE is made up of experts from 25 States: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, the Netherlands, Norway, Romania, the Russian Federation, Singapore, South Africa, Switzerland, the United Kingdom of Great Britain and Northern Ireland, the United States of America, and Uruguay. Their most recent final report was released on May 28, 2021.

In that report, the Group reaffirms that voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security, and stability. Also, that norms and existing international law sit alongside each other. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.

With respect to those norms, the Group noted that they "reflect the expectations of the international community and set standards for responsible State behaviour. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development."[12]

Given the unique attributes of ICTs, the Group reaffirmed their previous observation from a 2015 report that additional norms could be developed over time. Given this, it is useful to look at several of the norms enumerated to determine how those frameworks match up against reality.

Norm 13 (e) states that:

> States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

---

[11] Aaron Shull. 2013. Cyber Espionage and International Law. *GigaNet: Global Internet Governance Academic Network, Annual Symposium.*

[12] UN GGE. 2021. Report of The Group of Governmental Experts on Advancing Responsible State Behaviour In Cyberspace In The Context Of International Security.

It is hard to square this acknowledgement of a broad right to privacy in the digital age with the actual activities of the state actors, especially the more major powers, in question.

Much of the public debate, and outrage, flowing from the Snowden documents centered around a secret court order which allowed the NSA to collect the telephone records of millions of US customers. There were also disclosures of major "upstream" collection programs, BLARNEY, FAIRVIEW, OAKSTAR and STORMBREW, which were the code-names given to cable-intercept programs tapping traffic flowing into and across the US.13 There was also a large "downstream" program, called PRISM, which documents indicate had the NSA collecting data directly from Google, Facebook, Apple, Yahoo, and others.

However, the US is not unique in this regard. One can also point to several examples involving states such as Russia and China. In this regard, how then can states seek to enumerate a norm, while acknowledging that these are the expectations of the international community and standards for responsible State behaviour, and then continually breach them.

The answer is likely that they are not actually norms. A norm is defined as "a principle of right action binding upon the members of a group and serving to guide, control, or regulate proper and acceptable behavior."[14] However, there are misunderstood features of how norms actually work, which makes it possible to stigmatize actions that fall outside expectations as with, for example, 'rogue states.'[15]

The report from the GGE is riddle with other examples. Norm 13 (f) asserts that states 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. This while states are rushing to litter one another's electrical grids with malicious code, in case it is ever needed for either strategic or military reasons.[16]

Likewise, pursuant to Norm 13 (i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. One only need look to the discussion surrounding Huawei and 5G infrastructure to know that this "norm" is not likely being adhered to.

Furthermore, the second initiative underway at the UN is the open-ended working group. The open-ended working group, sponsored by Russia studies the existing norms contained in the previous UN GGE reports, identifies new norms, and studies the possibility of "establishing regular institutional dialogue ... under the auspices of the United Nations."[17] It is open to all 193 UN member states, and the open-ended nature means it could continue indefinitely.

---

[13] Ewen Macaskill and Gabriel Dance. 2013. NSA Files: Decoded. What the Revelations Mean for You. *The Guardian.*
[14] See Merriam-Webster dictionary definition.
[15] Mark Raymond. 2021. Confronting the Ubiquity of Norms in Cyberspace and Cyber Governance. *Lawfare*.
[16] See footnote 10.
[17] See UN GGE and OEWG

The existence of the OEWG exploring the same issues in a separate process reflects the fact that cyber norms have become an area of geopolitical rivalry. Support for the OEWG format fits within the broader global pushback against the notion that global powers have long determined the evolution of international norms.

Russia's latest resolution is to establish a committee of experts to consider a new UN cybercrime treaty, which would advance Russia's long-standing goal to replace the Council of Europe's Budapest Convention -the only international instrument addressing this issue. However, "the draft convention raises serious human rights concerns and the language in the resolution regarding what constitutes the use of information and communications technologies (ICTs) for criminal purposes is extremely vague."[18]

Ultimately, the distrust in international systems is substantial, and multilateral institutions are being weakened as a result. Cyberspace has become a central domain for international conflict requiring strategic collaboration amongst states. As David Sanger alludes to in the 'Perfect Weapon: War, Sabotage and Fear in the Cyber Age,' "cyberweapons are new, shrouded in secrecy, and invisible to the untrained eye, making them harder to comprehend than bullets or bombs."[19] The extreme degree of secrecy surrounding cyberweapons is excessive and nations are not prepared for the cyber-attack that is likely to come.

Attacks will most likely expand, and they will almost certainly accelerate. Sanger warns that there is virtually no chance that the hyperconnected and therefore target-rich Western democratic world will escape unscathed. With governments triggering ongoing cyberwars, imposing damage exceeding billions of dollars and crippling democracy, now is the time to have a much larger public conversation on the subject, before it is too late.

b) The influx of ransomware, data breaches and the tensions between:

Companies collect vast amounts of private information which have invariably become attractive targets for criminals. Just recently, McDonalds confirmed that hackers had stolen personal data from systems in the US, Taiwan, and South Korea. Information included customer emails, phone numbers and delivery addresses. This followed an incident where up to 3.3 million Audi and Volkswagen customers from the US and Canada were victims of a breach after their customer data records were stolen, including sensitive information such as social security and loan numbers. Furthermore, Air India has admitted to a massive data leak that compromised the personal records of about 4.5 million passengers. Proceeding this was an incident whereby a billion records belonging to the US health care and pharmaceutical behemoth that owns CVS Pharmacy and Aetna were exposed due to a misconfigured cloud service.

The rise in data breaches has revealed a dual threat, hackers are demanding a ransom to not only unlock the encrypted system but to also prevent further exploitation, such as the release of the

[18] Guest Blogger for Net Politics. 2020. A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet. *Council on Foreign Relations.*
[19] Elisabeth Eaves. 2018. David Sanger on the Perfect Weapon. *The Bulletin.*

private information to a wider audience. A recent occurrence involved multi-billion-dollar audio titan Bose, who refused to pay the ransom after attackers infected the company's network with ransomware and accessed (and potentially exfiltrated) human resources files relating to former employees.

In this regard, culprits will continue to step up efforts to steal money, information or otherwise monetize the value of stolen data assets. It is not news that the dark web, for example, is rife with offers of stolen data. Medical records, passport numbers, driver's licenses, credit card details, online banking logins, and social media credentials are readily used examples of information that are available through this avenue at disturbingly low prices.[20]

The barriers of entry into this lucrative criminal enterprise are shockingly low. Groups like the DarkSide, for example, are capitalizing on such extortion techniques, by operating like a franchise where individual hackers can pay a small fee to receive the attack software -packaged and ready for deployment.

Distributed denial-of-service attacks can be executed for as little as $500-700 USD.[21] Would-be felons do not need the technical skills to employ these malicious tactics since the crimeware kit includes simple instructions on how to execute an attack.[22]

The lack of geographic boundaries and anonymity that are characteristic of cyberspace also make it hard for states to identify exactly who is responsible. The challenge of tracing transactions through cryptocurrencies, generally stack the odds in the actor's favor. Regrettably, funds stolen from victims could very well be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction.[23]

Given the far-reaching consequences of the onslaughts, it can be challenging to also fully grasp the economic toll such attacks could take on an organization. However, a recent IBM security report highlighted that the global average price of a data breach in 2020 was approximately $3.86 million, while the healthcare industry had the highest average cost of $7.13 million. Recovering from the attack could take months, if not years. It is much more than just decrypting and restoring the data. Systems may need to be rebuilt, coupled with the operational downtown and the customer impact.

On top of this, a company's failure to secure data and lack of transparency surrounding how data is being used poses a continuous concern. A 2020 Cybersecurity Report released by the Canadian Internet Registration Authority (CIRA) -for example, surveyed more than 500 Canadian IT security decision-makers to learn more about their experience with cyber-threats. It

[20] For example, the cost of an individual's full credentials including, name, address, phone number, and social insurance number is as low as $8 per record. Online banking logins cost an average of $35 -at most. Full credit card details including associated data cost approximately $12-20. See Helpnet Security. 2020. How Much Is Your Data Worth On The Dark Web?
[21] Andrei Barysevich. 2017. Dissecting the Costs of Cybercriminal Operations.
[22] Institute for Security and Technology. 2021. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.
[23] Ibid.

found that only 36% of organizations informed a regulatory body after experiencing a data breach, down from 58% in 2019. And just 44% of those surveyed informed customers of a breach, representing a 4% decrease compared to 2019. In some ways, organizations are beginning to show compliance fatigue.

The widespread availability and collectability of data, on top of consumers' often passive willingness to share their personal information, has in some respect led to the increase in the velocity, visibility, and vastness of exposure. The irony is that most users expect that the infrastructure used to conduct their online affairs is secure enough to safely carry out those financial transactions; that their personal electronic health records are being sheltered from snooping eyes; that the information they access is reliable; or simply that the digital footprint left behind when using the Internet will not be used to inflict harm.

Citizens tend to be accustomed to trusting complex systems that they personally barely understand. It is now commonplace for a company's privacy policy acting as the means by which most consumers are given notice about what personal information is collected, for what purposes and with whom it is shared. These policies are often very long, complex, and legalistic. When one clicks "I agree" they may not know exactly what they have consented to and what is going to happen to their information. This has become an act of surrender rather than consent, and the growing commodification of user data threatens an already fragmented system that is rapidly eroding the confidence users have in the digital ecosystem.[24]

As a case study example, Canada's existing privacy laws leave consumers and organizations exposed to misuses of data mainly due to their outdated nature and the lack of enforcement power to protect citizens from data leaks and misuse. The proposed Bill C-11 the *Consumer Privacy Protection Act* (CPPA) offers greater enforcement powers to the Office of the Privacy Commissioner of Canada and introduces hefty fines to companies that breach its guidelines about the collection, use, and disclosure of personal information. Despite this, the bill continues to be in limbo at a pivotal time when Canada needs to get privacy right. It has also broadly been critiqued by experts on the basis that the legislation would not adequately address issues of meaningful consent, de-identification, or data mobility -among others.[25]

In the meantime, Canada's current lack of enforcement power continues to be highlighted. Recently the Federal Privacy Commissioner issued a joint report with provincial counterparts into Clearview AI's actions in Canada. Even with condemning the company's scraping of millions of Canadians' images from social media sites without consent, "the company rejected the commissioners' recommendations to stop collecting images of people in Canada and delete previously collected images and biometric details of individuals."[26] Public unease has also been

[24] The 2019 CIGI-Ipsos Global Survey on Internet Security and Trust involved 25,229 internet users in Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Republic of Korea, Russia, South Africa, Sweden, Tunisia, Turkey, and the United States. It found that 78% of global citizens are concerned about their online privacy.
[25] Teresa Scassa. 2020. Replacing Canada's 20-Year-Old Data Protection Law.
[26] Jim Bronskill. 2021. Clearview AI Facial Recognition Tool Broke Canadian Privacy Laws, Watchdogs Say. *Canadian Press.*

augmented by overt resistance to the Commissioner's rulings in instances like Facebook's defiant response to the Commissioner's findings regarding the Cambridge Analytica scandal.

Similarly, after the sensitive information of 15 million Canadians was exposed through a cyber breach at LifeLabs, Canada's largest laboratory-testing company, the Privacy Commissioners in Ontario and British Columbia conducted a joint investigation. It concluded that "the company failed to take reasonable steps to protect the personal health information in its electronic systems, failed to have adequate information-technology security policies in place, and collected more personal health information than was reasonably necessary." However, despite this, the commissioners noted they were limited in their ability to hand out an appropriate punishment.[27] A civil lawsuit has since been launched.

Nevertheless, high profile data breaches have left Canadians feeling vulnerable and unprotected. We are living in an age where data hungry companies are making fortunes from personal data that has weak legislative sanctions, highlighting that maintaining the status quo is not sustainable. Sufficient policy in all its aspects, not just public safety, is too important to be left solely in the hands of governments or, for that matter, private corporations -demonstrating the need for new norms, standards, and rules of behaviour via the multi-stakeholder model.

c) The growing ubiquity of the Internet and connected objects:

Connected devices are everywhere. They are emerging in every conceivable industrial sector where sensors can be embedded for vast data collection and analysis. For instance, "the total installed base of internet of things connected devices worldwide is projected to amount to 30.9 billion units by 2025, a sharp jump from the 13.8 billion units that are expected in 2021."[28] On top of this, the sheer volume of data that can be produced is astounding and will only continue to grow exponentially. For example, "the amount of data generated by IoT devices is expected to reach 73.1 ZB (zettabytes) by 2025. To put that in perspective – one zettabyte is 1021 bytes, [which means] one billion terabytes (TB) or one trillion gigabytes (GB)."[29]

With the rise of connected devices and associated data points, it is not surprising that the cybersecurity risks of IoT devices are well documented. Malicious operatives have subverted smart refrigerators, televisions, nanny cameras, digital assistants, doorbells, smart lighting, and thermostats -to name a few. Perhaps most problematic are the stories documenting the ease with which hackers can stop critical medical devices such as pacemakers and insulin pumps. This illustrates the fragility of today's digitally connected world.[30]

Indeed, one of the largest DDoS attacks in history, known as the Mirai Botnet, attacked major social media and content sites using hijacked IoT devices, such as security cameras and smart tv

[27] Xiao Xu, Laura Stone, Justine Hunter. 2021. Privacy Commissioners Slam Lifelabs for Failing to Safeguard Health Information. *Globe and Mail.*

[28] Statista. 2021. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025.

[29] Bojan Jovanović. 2021. Internet of Things statistics for 2021 – Taking Things Apart. *DataPro.*

[30] As an example, St. Jude Medical discovered a vulnerability existed in one of their implantable cardiac devices that could easily be exploited to adjust programming commands of the implanted device. Such manipulation could result in rapid battery depletion and/or administration of inappropriate pacing or shocks.

devices. The bot used a short list of 62 common default usernames and passwords to scan for vulnerable devices and surreptitiously infected them with malicious code. In essence,

> some connected home devices are not upgradable or come with inherently weak security. In other cases, owners ignore security patches as devices become part of the taken-for-granted background edifice of daily life. Consumer objects can be weaponized when they are vulnerable to exploits, and they are increasingly within crosshairs of those who seek to exert control across borders.[31]

On top of this, with ambient data gathering of routine activities, these devices are collecting information about everything we do, raising unprecedented privacy questions.

The reality is our economic model puts huge competitive pressure on companies to rapidly introduce products and services into markets. Consequently, we have installed strategic vulnerability into our digital ecosystem,

> by allowing poorly coded or engineered commercial-off-the-shelf 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.[32]

This has inadvertently engineered an easy path for cybercriminals since we have connected everything we possibly can to the Internet, and with the pace of cyber-physical innovation, it is clear public policy has yet to catch up.

In the absence of safety and cybersecurity regulations, "standards and certification represent the last line of defence to protect consumers, governments, industry and critical infrastructure from cybercriminals and state-sponsored cyberattacks."[33] But no discernible progress has been made in developing global cybersecurity standards focusing directly 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."

But as Michel Girard alludes to in his 2019 CIGI paper entitled *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter*,

> 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.[34]

Given the rise of the emerging attack surface we need a new approach to stimulate the development of global cybersecurity standards for IoT devices. In this environment, manufacturers of these technologies should be accountable for the digital security and safety of

[31] See page 6 of Laura Denardis. 2020. The Internet in Everything. *Yale University Press.*
[32] Melissa Hathaway. 2019. Patching Our Digital Future is Unsustainable and Dangerous. *CIGI.*
[33] Michel Girard. 2020. Standards for Cybersecure IoT Devices: A Way Forward. *CIGI*
[34] See Michel Girard. 2019. Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter. *CIGI.*

their products. Industries and standards bodies need to work together to create a unified cybersecurity strategy such as a comprehensive global standard that addresses product systems and processes around developing these devices, as well as their deployment.

d) The proliferation of disinformation and influence operations:

The manipulation of public opinion has also emerged as a critical issue impacting contemporary digital society. For instance, the whole edifice of democratic governance is based on a bedrock of values and standards. It is depicted as having an informed citizenry with a common sense of facts for informed public decision-making; facilitating a shared understanding of human rights and freedoms; and enabling a solid foundation for trust in the information provided by governments and institutions. However, this entire assemblage is being compromised by carefully crafted influence operations that seek to exacerbate divisions within society and breed distrust in the information environment and processes as a whole.

The prospective scale of influence operations is impacted by the array of digital platforms with vast numbers of users. Facebook has nearly 2.85 billion users. Twitter has 340 million. Mobile messaging applications that allow users to share threads and stories also capture huge proportions of the internet-using population, with 500 million Telegram users, 2.5 billion WhatsApp users and 1.2 billion Viber users, not to mention the many smaller messaging applications that exist.

The cloak of online anonymity that social platforms provide has enhanced their desirability to those who promulgate such influence operations, and this takes many forms. Whether its targeting politicians, political parties, or electoral processes to covertly influence public policy, public opinion or undermine democracy and democratic processes; or spreading conspiracy theories about QAnon; the 'infodemic' surrounding Covid-19; anti-vaxxers; or feeding political and religious extremism, actors are leveraging a range of readily available communication channels to propagate and amplify messaging, recruit others, and plan future pursuits. This is all taking place while social media companies seem perplexed that their platforms and algorithms have been weaponized and watch seemingly helpless while continuing to profit.

On top of this, an increasing number of cyber tools have been developed by state and non-state actors to assist in carrying-out these influence operations. For instance, in addition to attack vectors such as large armies of algorithmic bots, deepfake technology that relies on artificial intelligence and machine learning, has allowed for the creation of realistic-looking videos of events and public figures, adding an additional layer of uncertainty and manipulation. Concerns about the misuse of deepfakes to manipulate elections, propagate fraud in business, alter public opinion and threaten national security have dominated the discussions surrounding this technology.

Given the high level of sophistication, deepfakes pose a different level of threat, since they can be skillfully produced in such a way that even experts cannot say with certainty if they are real or not. This will greatly increase the qualitative impact of fake news and foreign influence operations, and as governments and researchers apply resources to understand how to tackle their

damaging use, it is critical that they pay attention to the people who are most commonly harmed by them.

While there may be no silver-bullet solution with respect to the disinformation problem, social media platforms have a fundamental role to play, and some are developing their own AI technology in an attempt to apply stricter policing and quicker action, to at least limit the impact. However, some form of regulation is also on the horizon. The unprecedented mob assault on the U.S. Capitol on January 6 represents perhaps the most stunning collision yet between the world of online disinformation and reality. Policy makers around the world, including those participating in the International Grand Committee on Big Data, Privacy and Democracy, continue to deliberate whether and to what extent platforms should be held accountable for the content they host, and the criteria that they should adhere to regarding accountability and enforcement.

Stricter laws and policies do have the potential to make a difference to curb the spread of harmful content, but they are only a start. Any efforts to contain disinformation should also address the broader social and media environment that leads so many people to take these messages seriously -this includes a greater push for digital literacy initiatives and awareness of the tools available to fight disinformation online.

To Conclude:

We are at a precarious moment in history, where the ongoing growth of interconnectivity is matched with the proliferation of cyber weaponry. There are four concluding points to be made: 1) the international rules-based system in cyberspace is still in its infancy, innovative thinking is needed to make sure that nations such as Canada can play a leadership role in crafting the governance architecture; 2) there is an extreme degree of secrecy surrounding cyberweapons in terms of their development and deployment and nations are not prepared for the degree of cyber-attack that is likely to come; 3) it is not just state actors that are launching attacks, the barriers of entry into this criminal enterprise are shockingly low. Malicious attacks techniques are sold online at a relatively small fee, meaning that attack mechanisms can be bought and deployed by anyone; 4) the public is now an increasing target for both criminal and state actors -spanning from ransomware attacks to data breaches to the spread of disinformation, which means that there is a need to foster a culture of cybersecurity awareness to manage risks and improve cyber hygiene practices.

While many of the complex policy challenges raised in this paper have no simple solution, these expanding threats cannot be stopped by piecemeal solutions that are deployed in a siloed, uncoordinated, or disjointed matter. Dependencies on the stability and security of cyberspace are not only vital to our digital economy and public sphere but are also now extended deeper into our human functioning. Essentially, "cybersecurity has now become one of the most consequential issues of the modern era, necessary for human safety, privacy, critical infrastructure, and national security, as much as for economic security, democracy, speech rights and access to knowledge." [35] Moving forward, states will need to better coordinate with respect to what the division of

[35] See page 7 of Laura Denardis. 2020. The Internet in Everything. *Yale University Press.*

authority and responsibility should be between public and private actors and different levels of government, all in an effort to increase international cyber stability.