02.06.2022
For discussion purposes only

Canadian Ditchley Foundation
Fondation Canadienne Ditchley

DIGITAL SECURITY FOR ECONOMIC AND SOCIAL PROSPERITY[1]

The Canadian Ditchley Foundation's 2022 Biennial Conference, in collaboration with the University of Ottawa, will be held November 3-6 at the Château Laurier. The conference will bring together an international group of leading thinkers and practitioners from business, finance, national security, law enforcement, government and academia to discuss ways and policies to strengthen digital security for all of society. We want to enable a candid and protected conversation, creating a rare opportunity to develop shared strategic thinking aimed at ensuring that digital technologies better serve the common good.

In preparation for the Canadian Ditchley Foundation's 2022 Biennial Conference, this paper provides a brief overview of the nature and scope of threats to digital economic and social security, the initiatives being taken at the national and international levels to bring some order to cyberspace, and the daunting public policy challenges that will be posed in the future by runaway developments in digital technologies.

- THE UNFOLDING DIGITAL REVOLUTION

Over the past 30 years, the Internet and other digital technologies have become essential for the functioning of governments and public and private organizations in the conduct of their core activities. The ongoing digital revolution is transforming virtually every aspect of society at an accelerating pace, making individuals of all ages as well as organizations increasingly dependent on digital technologies. The rapid spread of mobile devices, cloud computing, Internet of Things, edge computing and data analytics is a key feature of this revolution - and one of the drivers of this acceleration. These developments have made the world denser with flows of information, knowledge and trade, including the expansion of markets and the mobility of capital in ways that produce wonders and woes.

Digital technology has been beneficial to human progress, bringing significant improvements to the lives of people around the world, including recent and rapidly deployed technologies in health, workplace and agriculture, manufacturing and commerce. Certainly, online platforms have played a critical role in helping citizens and businesses overcome the disruptions caused by Covid-19, supporting distance learning on an unprecedented scale, enabling work-from-home for much of the workforce. Widespread consumer use of the internet has somewhat mitigated the negative impact of the pandemic, albeit unevenly.

In healthcare, digital technologies have been leveraged to support the public health response to COVID-19 worldwide by dramatically improving digital epidemiological surveillance, rapid case identification, and real-time public health data collection to help policymakers refine interventions, it being the case for Ebola and Covid-19, and by bringing efficacy to the delivery of vaccines to hundreds of millions in an orderly and traceable manner.

[1] The Ditchley conference will focus on digital security issues that are primarily business, economic and societal in nature and generally exclude aspects such as the role of ICTs in intelligence, conflict prevention, warfare, etc. We recognize that the different dimensions of digital security (economic, social, technical, law enforcement, national and international security) are interdependent; therefore, governments should strive for coherence, complementarity and enhanced synergies in the design and implementation of digital security policies.

Advances in genetic engineering technology, enabled by ever-increasing computer processing speed, DNA sequencing, and advanced analytics, have allowed the rapid and inexpensive production of new vaccines, as evidenced by Covid RNA vaccines, and the "repair" of human genetic diseases, such as the treatment of blood disorders like sickle cell anemia and other genetic diseases like muscular dystrophy. These same technologies have led to amazing advances in agriculture, enabling early detection and response to diseases and threats. Other digital technologies perceived as commonplace today include the GPS and digital payment applications that have revolutionized the way businesses and consumers send and receive money. Also consider machine translation, which is now available in real time on smartphones. Apps don't just translate text; they are able to instantly translate speech, overcoming the language barrier that hinders communication between people who speak different languages.

The digital revolution has so far been characterized by a shift in power from public institutions to private actors and the technologies they control. Taking full advantage of the ubiquity of the mobile internet, and developments in IT technologies such as virtualization which enables applications to be separated from the infrastructure; the significant reductions in data storage costs and the automation of maintenance tasks once done manually; the emergence of high-performance GPUs (graphic processing units) that can perform sophisticated predictive computing and analysis at very high speeds; artificial intelligence and machine learning, info tech companies are transforming societies and the global economy on a perhaps larger scale than the second Industrial Revolution. Seven of the world's top 10 companies by market capitalization are info tech titans: Apple, Microsoft, Amazon, Alphabet, Meta Platforms, Alibaba and Tencent. Their prominence, economic heft, and the momentous social impact of the digital tools they make available to so many raise difficult new policy and governance issues that remain largely unresolved.

We must recognize that tools created with the best of intentions can cause unexpected problems and that digital technology cannot provide an escape from our "residence on earth." Alongside the good and extraordinary opportunities for innovation and growth that the Internet and other digital technologies offer, they have created three major waves of negative externalities.

The first was and remains the pervasiveness of cyberattacks that exploit the vulnerability of institutions, businesses, and governments through extortion or hacking for political purposes, the disabling of organizations' computers, repeated episodes of data breaches, theft of intellectual property and trade secrets and attacks on critical social and economic infrastructure. As the number of Internet connections has grown, and continues to grow exponentially, the surface area vulnerable to cyberattacks has expanded dramatically.

The second wave of negative externalities stems from the current structure of the internet which can be quickly exploited to spread misinformation, disinformation, and hate, while the third wave comes in the form of internet surveillance, which allows companies to amass huge amounts of user profiles and behavioral data, conduct data mining, and sell personal information to be used as raw material to not only predict but also modify the future behavior of individuals and consumers.[2]

The vulnerability of public and private organizations to cyberattacks, the increasing pervasiveness of misinformation and disinformation campaigns, and the inability of individuals to control their own digital lives paint a disturbing picture of a cyberspace in chaos. This anarchic situation creates a profound sense of vulnerability that undermines trust, a fundamental ingredient of social capital, and threatens the social fabric.

[2] Tim Cook, *It's time for action on privacy: we all deserve control over our digital lives*, TIMEs, January 28, 2019.

- PROMOTING A SAFE AND SECURE DIGITAL ENVIRONMENT

The domain of cyberspace is inherently transnational. Among its special characteristics are the reduction of distances, the speed of interactions, the low cost - which reduces barriers to entry - and the difficulty of attribution which favors denial.

A key challenge in developing digital security policy in cyberspace-dependent democratic societies is to foster economic and social prosperity and human well-being while managing digital security risk in a manner that preserves the openness of the Internet as a platform for innovation and new sources of growth.[3] The difficulties are compounded by the fact that the pace of change in the cyber domain is explosive, while our mindsets and institutions are geared toward gradual linear change.[4] There is growing international recognition that governments must treat digital security risk as an economic and societal rather than a technical issue. Therefore, to be successful, a strategy must avoid a techno-deterministic approach and address digital security in an integrated and comprehensive manner that encompasses:

i. a legal and regulatory framework designed to protect important social values and the rights of users, and, henceforth, maintain confidence and trust in cyberspace activities. The regime must include basic requirements that public and private stakeholders must meet and legal instruments prohibiting harmful actions, as well as the means to enforce such rules and prosecute failures to conform to legal requirements;

ii. an apparatus to identify and counter domestic and foreign cybersecurity threats, strengthen resiliency and mitigate their economic, political and social disruptive impacts;

iii. internationally accepted legal frameworks governing cyber operations, international data flows and digital trade; and

iv. an education system that integrates digital literacy and critical thinking for all students, at both secondary and post-secondary levels.

The ability to collect huge amounts of data is a double-edged sword. On the one hand, it empowers governments, businesses, and individuals to make better decisions. On the other hand, it raises big questions about how that data can be used while protecting people’s right to privacy. The salience of the issue is compounded by the growing number of massive data breaches exposing personal data, and in some cases leading to financial fraud and identity theft, is causing concern among individuals who are often left to fend for themselves. These concerns have led to legislative action to address the situation. The European Union's General Data Protection Regulation (GDPR) is the most comprehensive privacy legislation currently in place. The regime governs how personal data of EU and EEA residents may be processed and transferred. The GDPR rules are supplemented by measures to ensure that protection is maintained when personal data leaves the region. In Canada, Bill C11 first brought forward in 2022, is back on the table. If adopted, the legislation would significantly modify the current Privacy landscape and would bring Canada closer to the European regime.

The International Telecommunication Union reports that, as of 2020, 133 countries have written protection and privacy regulations into law, 102 countries have adopted data breach and incident reporting requirements, and 97 have legislation on illegal access, online identification, and data theft. For instance, in the U.S.A. operators of critical infrastructure are now required to report any security breaches.

[3] Katharina Lima de Miranda, Dennis J. Snower, *Recoupling Economic and Social Prosperity*, IZA Institute of Labor Economics, IZA DP No. 12998, February 2020.

[4] Scientists define an explosion as the injection of energy into a system at a pace that overwhelms the system’s ability to adjust. This seems to be a good description of the disruptive effects of the development of digital technologies..

Table 1 shows the global scores and rankings for selected countries in 2020 on these dimensions.

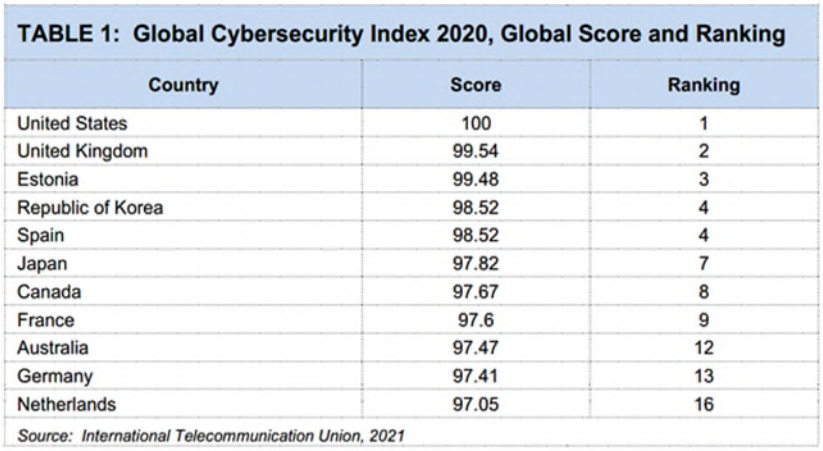


TABLE 1: Global Cybersecurity Index 2020, Global Score and Ranking

Country	Score	Ranking
United States	100	1
United Kingdom	99.54	2
Estonia	99.48	3
Republic of Korea	98.52	4
Spain	98.52	4
Japan	97.82	7
Canada	97.67	8
France	97.6	9
Australia	97.47	12
Germany	97.41	13
Netherlands	97.05	16

Source: International Telecommunication Union, 2021

From a societal perspective, the pervasive impact of digital technologies is causing countries to adopt more forceful policies aimed at eliminating its socially debilitating manifestations. The relatively recent evolution of online child protection policy such as the United Kingdom's Age Appropriate Design Code regulation that impose tighter restrains on social media companies, video streaming and gaming platforms practices,[5] the proposed legislation to strengthen online safety protections for children being considered by the U.S. Congress and the California state legislature are cases in point. President Biden's call to "strengthen privacy protections, ban targeted advertising to children, and require technology companies to stop collecting personal data on children" is another illustration of the social importance of the issue. This new focus of policy-making stems from the recognition that the age-related risk profile has changed, with the use of mobile devices with mobile internet connections increasing among the very young since 2012. On March 17, 2022, the United Kingdom took another step forward with the introduction of the *Online Safety Bill* in Parliament. This bill addresses a wide range of issues from online fraud to child sexual abuse and places a duty on platforms, among several other responsibilities, to remove content deemed "legal but harmful."

The task is not finished. The rampant spread of hate speech, incitement to violence, online gender-based attacks in the form of harassment, identity theft, stalking, sexual slurs and images, forgery, and surveillance continues, thanks to the lackadaisical efforts of digital network platforms and governments to address the issue. Individuals of all ages are encouraged to engage and play in "parallel universes" where there are essentially no rules, no regulation, and where reprehensible language and behaviours circulate in total impunity. The Financial Times recently reported a disturbing incident where the avatar of an academic playing in the "Facebook metaverse" was groped.[6] If such behavior is not acceptable in real life, why should it be acceptable in virtual space?

- **CYBERSECURITY CONCERNS**

It is generally accepted that a secure digital environment is a prerequisite for an effective national digitization effort which is critical to sustain innovation and competitiveness. Business leaders are increasingly concerned about cyber threats. According to several surveys, cyber-attacks are among the most severe and likely risks facing businesses and government leaders in advanced economies especially for financial service firms which may experience up to 300 times more cyberattacks per year than other firms.[7] Close to half of the senior experts consulted by the Bank of Canada share the view that the potential for a cyber incident is the largest risk that could harm individual firms and the financial system as a whole.[8] In the United Kingdom, 61 percent of respondents to the latest Bank of England's Systemic Risk Survey stated that cyber-attacks was the main source of risk to the UK financial system.[9] The vulnerability of banking institutions is increased by the proliferation of interconnected devices, digitalization of banking, and

[5] *Protecting Children Online : An overview of recent developments in legal frameworks and policies*, OECD Digital Economy Papers, May 2020, no. 295.

[6] Financial Times, *Full Disclosure: What the legal world is reading this week*, 23 February 2022.

[7] Thomas M. Eisenbach, Anna Kovner, Michael Junho Lee, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, Federal Reserve Bank of New York, Staff Reports, no. 909, January 2020, revised May 2021.

[8] Bank of Canada, *Financial System Survey Highlights*, November 2020.

[9] Bank of England, *Systemic Risk Survey Results*, December 2019.

remote working that provide new entry points for attackers. In the U.S., between 2016 and 2020, approximately 25 percent of cyberattacks against industry targeted financial institutions. More broadly, 39 percent of respondents in the Global Risk Report forecast that cybersecurity failure presents a *clear and present danger* to the world within the next two years.[10]

Cyber events, both large and small, ranging from breaches that could corrupt their own data or make confidential information public, to denial of service and ransomware that has metastasized into an increasingly common type of cyber incident, have significant economic and social consequences for public and private organizations and individuals.

BOX 1: Examples of large-scale cyber incidents

Years	Incidents
2013	U.S. retailer Target was hit during the Christmas sale season. 40 million credit and debit card numbers and over 110 million customer records were stolen.
2014	U.S. retailer The Home Depot was confronted with the theft of 56 million pieces of credit and debit card information.
2014	U.S. bank JP Morgan Chase faced the theft of information for nearly 76 million American households and 7 million small businesses.
2014	In-depth intrusion of Sony Pictures Entertainments' networks led to widespread public exposure of internal communications and personal data of employees and partners, as well as yet to be released movies.
2017	The ransomware attack targeting the Microsoft Windows system has infected approximately 200,000 computers in 150 countries with the virus called WannaCry. National Health Service hospitals in England and Scotland, with up to 70,000 medical devices, are estimated to have been affected. The attack also crippled production at Nissan Motor Manufacture and Renault in the UK. Telefonica and FedEx in Spain were also affected, as well as many organizations around the world.
2021	The hack that shutdown the Colonial Pipeline, an important piece of U.S. critical infrastructure, disrupted gas supplies to the entire U.S. East Coast, causing chaos and panic.
2021	By exploiting a vulnerability in a Microsoft Exchange server, hackers gained access to Taiwan Acer files and leaked images of sensitive financial documents and spreadsheets.
2021	IBS Foods, one of the world's largest meat processors, was the subject of a ransomware attack that cost it $11 million in ransom payments.
2021	AXA, the French insurance company, was subject to an attack in which hackers gained access to a massive amount of data (3 TB).
2021	U.S. insurer CNA Financial suffered a ransomware attack that disrupted the company's employee and customer services for three days. The personal data of more than 75,000 people was exposed in the attack. CNA Financial paid a ransom of $40 million.
2022	A large-scale ransomware attack crippled 17 European oil port terminals, causing tankers to be diverted and significantly disrupting supply chains and the availability of refined products.

Future events could be far more disruptive than the cyber events listed above. For example, it was recently revealed that Russia has developed malware designed to disrupt power grids. *CrashOverride*, which knocked out part of the power grid in Ukraine, has been significantly enhanced and appears to have been specifically designed to be deployed against European and North American power grids.

Yet, large-scale cyber incidents are only the "tip of the iceberg." According to the Canadian Cybersecurity Centre, "in the first half of 2021, global ransomware attacks increased by 151% compared to the first half of 2020," while acknowledging that most attacks go unreported, in part due to the stigma of cyber incidents. Indeed, studies show that an average cyber incident reduces a company's share prices by 5 to 7 percent.

[10] World Economic Forum, *The Global Risk Report 2021*, January 2021.

Despite the severity of their crimes, the majority of ransomware perpetrators operate with virtual impunity, from nation-states that are unable or unwilling to prosecute these cybercrimes. This problem is exacerbated by the fact that ransomware is paid with hard-to-trace crypto-currencies. Cybercrime is becoming extremely sophisticated and requires equally sophisticated detection and investigation capabilities. National governments in democratic countries will not be able to stem ransomware attacks by rogue states or foreign criminal gangs by "playing defense" or offloading the problem on the private sector. It is the responsibility of the state to protect its sovereignty. In the realm of lawlessness, the policy response must give a much greater role to the use of offensive cyber forces to attack and disrupt cyber criminals and recover ransom money.

The complex nature of the threat requires governments to take a comprehensive approach to deterring ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; to disrupt the business model and reduce criminal profits; to help organizations prepare for ransomware attacks; and to respond to ransomware attacks more effectively.

Concerns about data security and privacy risks often lead to hesitations by senior business executives in taking the decision to move to cloud computing. The importance of this issue has prompted the European Network and Information Security Agency (ENISA) to look into this aspect. Their main conclusion is that, although cloud computing involves a large concentration of resources and data, "cloud-based defenses are more robust, scalable and cost-effective". One of the strengths of cloud computing comes from the fact that its performance depends on an architecture where (i) computing resources are abstracted from the underlying hardware; (ii) data from independent customers sharing hardware and software resources is protected by logical isolation mechanisms; (iii) not only is the data in transit and "at rest " encrypted but, with the emergence of confidential computing, it is encrypted in use during computation, and (iv) storage and processing of computing content is massively distributed. The European Commission has reached a similar conclusion stating that "contrary to the belief that using public cloud resources would reduce the security posture of the European Commission, reality has proven that a correct usage of public cloud resources can actually increase the overall security resilience by removing internal risks" (European Commission, 2019).

- The Specter of Information Disorder

> *"One uses information to destroy nations, not networks"*
>
> *General Nikolai Makarov*

Trust is a basic ingredient of social capital; it plays a central role in societies because it fosters cooperation among individuals, it underpins development, security, stability, confidence in the financial markets and it facilitates productive activity in organizations of all sizes by reducing risk and the need to spend scarce resources to accumulate information about their counterparts, thereby promoting prosperity. [11] Trust and other cultural virtues can be destroyed more easily than created. Digitally dependent democratic societies are particularly vulnerable to malignant cyber operations aimed at manipulating social networks and relationships that fuels anomie, thereby causing a breakdown in trust. Social media campaigns by government sponsored, ideologically driven or conspiracy minded "hacktivist" groups that question the integrity and legitimacy of a government - for example, the results of an election - or that divide communities into clustered networks living in "echo chambers" and parallel information universes, spread suspicion and unleash the kind of forces that forment civil unrest and threaten democracy.[12] A worrying dimension of this

[11] Francis Fukuyama, *Trust: The Social Virtues and The Creation of Prosperity*, The Free Press, 1995. See also Alain Peyrefitte, *La société de confiance: Essai sur les origines et la nature du développement*, Édition O. Jacob, January 1, 1995.

[12] *Les lumières à l'ère numérique*, Rapport de la Commission, République Française, Janvier 2022.

phenomenon is that research shows that misinformation and hate speech are intimately linked in practice: false and misleading information fuels hate speech and vice versa. The pervasiveness of the phenomenon should not be underestimated: in the first quarter of 2021, Facebook removed nearly 10 million pieces of hateful content, compared to 6.4 million at the end of 2020. This raises a question: what if social media users were to be identifiable in real life?

Disinformation is not like pornography; large segments of the population do not know when they see it. While people agree that disinformation is a problem, countering these harmful threats to the foundations of democratic societies, social institutions and business interests is made difficult by the facts that large surveys have found that (i) social media which depend on a vast array of users to generate relatively unfiltered content is the primary source of information for many people, and (ii) most people seek perspectives they already agree with, turning their social media feeds into echo chambers from which they don't try to escape. This has the effect of distorting the consumption of information and the identification of truth, leading people to let their capacity for independent reasoning and judgment atrophy. This effect is compounded by the fact that fake news is 70 percent more likely to be retweeted than real news and the modus operandi of social media platforms that are designed to multiply clicks by generating outrage which, in turn, generates advertising revenue. The fact that democratic governments rely on digital network platforms to set community standards for what content is permissible to create and share and enforce the policy through the removal of objectionable content and accounts, highlights the incongruity between the modern digital space and traditional norms, rules and expectations.

The disastrous consequences for democratic institutions, organizations and individuals of digital-based disinformation and conspiracy theories on social media are drawing increasing attention. According to the U.S. Aspen Institute's Commission on Information Disorder, the United States "is in a crisis of trust and truth". Its scalding report states unequivocally that "bad information has become as prevalent, persuasive, and persistent as good information, creating a chain reaction of harm. Information disorder is a crisis that exacerbates all other crises. It makes any health crisis more deadly. It slows down response time on climate change. It undermines democracy." [13] It's interesting - and concerning because it's medical misinformation - that as of April 2021, Facebook said it had removed 18 million Covid-19-related misinformation posts, in addition to the 167 million Covid-19-related posts it classified as "fake or false." In a similar vein, the Digital Forensic Research Lab (DFR Lab) has documented competing and contradictory narratives about the origin and spread of Covid-19 disseminated internally and externally by China, Russia, Iran and the United States.[14] The blame rhetoric's have contributed to a loss of public trust, making it difficult for health officials to implement sound policies and preventing multilateral cooperation in the fight against the pandemic.

Disinformation is both a national and an international problem. It can be created and disseminated by domestic actors, or created abroad and transferred between malicious actors from one country to another. The severity of the threats is heightened by the fact that domestic actors mimic the tactics used by foreign actors. For example, it has been observed in the European Union that inflammatory narratives on divisive topics such as "immigration/migration, anti-religious sentiment (Muslim and Jewish), nationalist identity, women's health, gender-based harassment, and climate change" are being disseminated and amplified across national borders by domestic and international actors to mobilize regional and international communities.[15] Another case in point is the relaying by right-wing American news sites (e.g. Infowars), podcasters and commentators of Kremlin claims that the invasion of Ukraine was necessary to protect Russia from biological weapons developed in U.S.-funded Ukrainian laboratories. This bioweapons

[13] *Commission on Information Disorder Final Report*, Aspen Institute, November 15, 2021.

[14] DFR Lab, *Weaponized: How Rumors about Covid-19's Origins Led to A Narrative Arms Race*, February 2021.

[15] *Open data analysis – European Parliamentary Elections: Comprehensive Report* (https://www.international.gc.ca/gac-amc/publications/rrm-mrr/european-elections-europeennes.aspx?lang-eng?lang=eng&lang=eng), Global Affairs Canada (GAC) (Report), August 2, 2019.

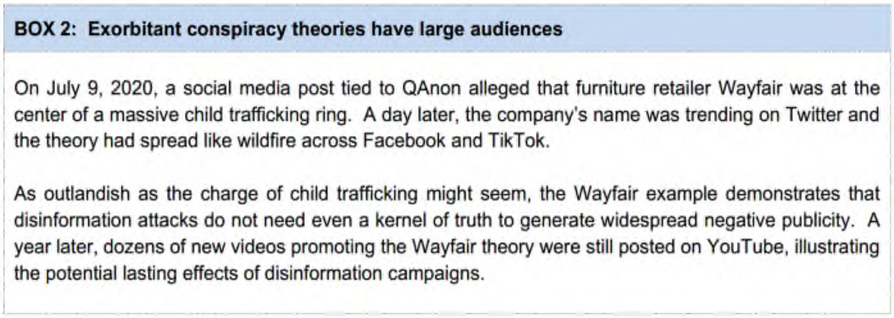
conspiracy theory has been growing in American online forums, blaming Putin and the Kremlin's invasion of Ukraine on NATO, the U.S. government and President Biden's administration.

Faced with these challenges, democracies are limited in the range of measures they can deploy to mitigate the impact of insidious cyber-influence and propaganda operations aimed at shaping, subverting and confusing public opinion bound has they are by their attachment to fundamental rights such as freedom of speech while, on the contrary, autocracies that don't care are assisted by cyber technologies. Moreover, because of its global and continuous characteristics, disinformation is a 'wicked problem' that transcends countries and generations. Nevertheless, remedies to the current state of affairs in the digital public sphere that appropriately balance rights, safety and dignity can be adopted. For example, the Canadian Criminal Code provisions against hate speech are based on the principle that "in a democratic society, freedom of expression does not mean the right to vilify. " Sweden went a step further by establishing the Psychological Defence Agency within its Ministry of Justice earlier this year. Focusing on external threat actors, the Agency aims to preserve democratic society and free opinion formation. The Agency's modus operandi is modeled on that adopted in the fields of consumer protection and epidemiology.

Sophisticated AI-based disinformation attacks will only increase in aggressivity and frequency. For example, deep-fakes - fake digital images, videos, or audio generated by AI - are increasingly being used to impersonate individuals, politicians, senior business executives, and opinion leaders. With automated disinformation capabilities and natural language processing, we should soon expect deep-fake campaigns to soon proliferate and be conducted at scale.[16] As "disinformation technology" becomes more sophisticated, it is giving rise to a new industry where malicious actors can hire "disinformation services" and buy the services of professional-grade forgeries that will conduct a targeted disinformation or deep-fake campaigns for a fee. Confronted with waves of nefarious disinformation, industries, governments and law enforcement agencies need technological tools, beyond the basic cybersecurity tools, to meet the challenge.

- Corporate Brand and Reputational Risk

Business leaders must disillusion themselves of the idea that disinformation and misinformation are means of political warfare, not directly relevant to their business. There is ample evidence that disinformation campaigns aimed at target companies are on the rise. Digital attacks are inconspicuous as they are insidious. With the polarization of public opinion in Western societies, large corporations are "soft targets" that can be drawn into "culture wars" as a result of false information from online conspiracy theory or ideology-minded generators. Misinformation concerning a brand or a corporation can be devastating and long-lasting.



BOX 2: Exorbitant conspiracy theories have large audiences

On July 9, 2020, a social media post tied to QAnon alleged that furniture retailer Wayfair was at the center of a massive child trafficking ring. A day later, the company's name was trending on Twitter and the theory had spread like wildfire across Facebook and TikTok.

As outlandish as the charge of child trafficking might seem, the Wayfair example demonstrates that disinformation attacks do not need even a kernel of truth to generate widespread negative publicity. A year later, dozens of new videos promoting the Wayfair theory were still posted on YouTube, illustrating the potential lasting effects of disinformation campaigns.

This gives rise to an entirely new set of risks, creating a highly charged environment in which vulnerability to coordinated disinformation and misinformation attacks now poses a serious threat to brand equity, stock price, employee relations, corporate culture, customer trust and the physical safety of executives. To combat this phenomenon and avoid being caught off guard, companies must commit to building defense capabilities and invest in resources that can perform real-time analysis and forecasting. There is also an urgent need to develop skills in the area of disinformation and misinformation defense expertise.

[16] Ben Buchanan et al, *Truth, Lies, and Automation: How Language Models Could Change Disinformation,* Center for Security and Emerging Technology, May 2021 (Georgetown.edu), 35-37.

The ability to detect and predict emerging coordinated and inauthentic cyber social and economic threats is gradually being enhanced by some major initiatives. The Network Contagion Institute (NCRI) has developed a proprietary platform to study social media feeds, publicly available community data, and personal survey information in near-real time with unprecedented accuracy and predictive power. Located at Rutgers University, NCRI has established a formal collaboration with the world's leading universities that have been given access to its proprietary ingestion engine to further track and study the phenomenon of misinformation and disinformation and to share expert knowledge.[17]

> *"By failing to prepare you are preparing to fail"*
>
> *Benjamin Franklin*

- THE GOVERNANCE OF CYBERSPACE

The lack of sensible governance of cyberspace and failure to abide by international law applicable to cyber operations invites excess and gives rise to systemic risk of unfathomable proportion.

The ever-increasing spread of digital technologies and connectivity in our economies means that the risk of cyber incidents is a question of when, not if. It is impossible to create a "safe and secure" digital environment where risk is completely avoided, except by eliminating digital openness, interconnectedness, and synchronicity, and by foregoing the economic and social benefits that these properties can unleash. Planning for resiliency and educating staff on digital hygiene is a good start. Companies and institutions in strategically important sectors are in the crosshairs of hackers of all stripes. Like any risk, the threat of cyberattack must be managed, and given the amount of damage a successful penetration can cause, it requires the attention of the CEO and senior management. However, in light of the geopolitics of cyberspace - the vast majority of cyberattacks against Western countries, whether by criminal groups or state-sponsored actors, emanate from China, Iran, North Korea, and Russia - "outsourcing" primary responsibility for digital security to the private sector is not an appropriate nor an effective defense and deterrence policy. Despite the rapid growth in cybersecurity spending by businesses to bolster their cyber defenses and the resilience of their ICT systems, the number and scale of ransomware and other cybercrimes are increasing at an accelerating rate. This has led a group of technology companies and law enforcement agencies from the U.S., U.K. and Canada to advocate for aggressive international action to combat ransomware, including punishing countries that fail to crackdown on the problem.

The effectiveness of digital security policies is further hampered by the lack of national bodies responsible for collecting and reporting timely and comprehensive information on current cyber threats to industries or organizations that may be targeted. Such information would include detailed data on larger-scale cyberattacks that tend to spread across industries; the security record of current technologies; the effectiveness of certain defenses and the relative benefits of different security measures; and the relative security and vulnerabilities of common software products that give hackers the ability to exploit a single vulnerability to penetrate a large number of targets. Much of this information is known, but carefully guarded by cybersecurity companies and cyber insurers. Creating an information sharing organization to fill the existing information gap is an appropriate government responsibility.[18] An open question is whether this sharing of information should be mandated by law, or kept voluntary. In addition, as recommended by the OECD, there is an urgent need to close the digital security gap inherent in "smart digital products", which too often lack an adequate level of digital security, by implementing "smart policies for smart products".

[17] NCRI partner universities include Rutgers, Massachusetts Institute of Technology, Stanford University, Northwestern University, University of Oxford, Princeton University, Yale University, University of Ottawa and James Madison University.

[18] In the United States, the Federal Aviation Administration established the Aviation Safety Information Analysis and Sharing (ASIAS) program, which is now considered the aviation industry's most valuable source of safety information and has contributed to a substantial reduction in fatal air accidents in the United States.

The *Cybersecurity Improvement Act* adopted by the U.S. Congress and other guidelines for cybersecurity, device identity and encryption that provide an additional compliance layer that forces OEMs in other industries like medical devices, automotive and critical infrastructure, to design secure products to support vulnerability reduction during operation should be emulated by other countries. International cooperation is necessary to enable interoperability between national approaches, avoid proliferation of standards and limit inconsistencies between jurisdictions.[19]

- FOSTERING INTERNATIONAL ORDER IN CYBERSPACE

Recognition of the need for international rules and cooperation in dealing with cyberspace issues has gained ground, particularly in the areas of cybersecurity and e-commerce. The EU's cybersecurity policy states that there is "a need for closer cooperation at a global level to improve security standards, improve information, and promote a common global approach to network and information security issues…"[20] The most recent U.S. Cybersecurity Strategy reaffirms the need to "strengthen the capacity and interoperability of those allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats",[21] a conclusion that forms a major thrust of Canada's National Cyber Security Action Plan.[22] In March 2021, UN Working Group comprising all 193 member states adopted a consensus report on norms for responsible state behaviour in cyberspace.

It is somewhat paradoxical that the UN report originated with a Russian proposal! History shows that the key to international order lies in respect for the "rule of law" which, among other obligations, requires that: "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States. " [23]

Skeptics are quick to dismiss the importance and role that standards can play in bringing about a new digital order. Joseph Nye Jr. addresses this issue by stating that: "Norms create expectations about behavior that make it possible to hold other states accountable. Norms also help legitimize official actions and help states recruit allies when they decide to respond to a violation. " [24]

- MAKING THE MULTILATERAL TRADING SYSTEM FIT FOR THE 21ST CENTURY

The defining feature of the digital economy is its focus on intangibles – data and knowledge – rather than things. And because data is a non-rival, it can be replicated and reused over and over again to make connections within and across industries feeding in the process the exponential growth in the volume of data to ingest, store and process, and the creation of new enterprises, services and industries built on cross-border know-how flows.

With the advent of cloud platforms and other data-driven enabling technologies, such as artificial intelligence, data from one country is increasingly being stored, processed and analyzed in another. While the existing multilateral trade agreements underpinning the WTO (GATT, GATS, and TRIPS) provide some common principles for regulating the provision of e-commerce services, but the lack of a full-fledged multilateral framework governing these cross-border flows provides fertile ground for the coalescence of a digital divide, which does not allow for economies of scale and scope in data, leading to fragmentation of digital business transactions. Divergent or obstructive standards, data localization or technology supply requirements, and excessive national security protections are not conducive to healthy evolution, as they undermine the ability of data flows to drive growth and well-being. In this regard, the July 2020 ruling by

[19] OECD, *Enhancing The Digital Security of Products: A Policy Discussion*, February 2021, No. 306.

[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of framework and information systems across the Union.

[21] White House National Cybersecurity Strategy, September 2018.

[22] Public Safety Canada, *National Cyber Security Action Plan: 2019-2024*, 2019.

[23] *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Second Edition - Cambridge, prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

[24] Joseph S. Nye, Jr., *The End of Cyber-Anarchy? How to Build a New Digital Order,* Foreign Affairs, January/February 2022 issue, pp. 32-42.

the Court of Justice of the European Union (CJEU) invalidating the EU-U.S. Privacy Shield framework, which was the primary vehicle for enabling transfers of personal data from the EU to the U.S, has not only created major obstacles to the continued flow of important data across the Atlantic, but it has also created uncertainty for many of the EU's trading partners - including Britain and Canada - and for all EU businesses involved in international trade.

The implications of the Court's ruling on Trans-Atlantic data flows led the United States and the European Commission to resume negotiations, culminating in the March 25, 2022 announcement of the parties' commitment to a new Trans-Atlantic Data Privacy Framework that will re-establish a legal mechanism for the transfer of personal data from the EU to the United States. This latest development is consistent with the ongoing WTO negotiations, involving 86 members, to reach an agreement on new common rules for trade-related aspects of e-commerce. The G7 could push for accelerating e-commerce negotiations and look for common ground on rules that ensure connectivity and interoperability of digital markets facilitate digital trade, improve transparency through the adoption of a taxonomy, including different types of data, and provide legal certainty.

- A CHALLENGING DIGITAL FUTURE IN PERSPECTIVE

> *"If you think this has a happy ending, you haven't been paying attention"*
>
> *Game of Thrones*
> *(comments by the fictional character Ramsay Snow)*

The runaway pace of development and deployment of new digital technologies is likely to accentuate and increase the negative externalities associated with the current generation of digital technologies, creating a daunting challenge to ensure digital security for and within democratic and open societies. On our doorstep, we have:

- **5G technologies:** The fifth generation of wireless networks and technologies (5G) presents significant opportunities to transform connectivity improvements in bandwidth, coverage and reliability, enabling a range of enhanced and new applications. The ultra-reliable low-latency capability, ultra-high bandwidth, and service reliability of 5G will drive industry innovation and a massive expansion of IoT, life support, and other internet-connected devices, creating an exponential increase in the amount of information and data access. With these innovations come additional digital security and risk challenges. Because 5G deployment involves the conversion of current physical communication networks to a primarily software-only network and the vast expansion of bandwidth that make 5G possible, fifth-generation networks will be inherently more vulnerable to multi-dimensional cyberattacks.

- **Quantum technologies** will likely impact digital security in three distinct ways:

1. The immense computing power of quantum computers will enable the analysis of cyber and privacy data to detect anomalous or suspicious behavior.

2. Their physical properties will enable the development of improved components for cyber systems such as cryptographic key generation and distribution.

3. As quantum computing advances, solving Shor's factorization algorithm will make most encryption techniques easier to crack, making data and transactions more vulnerable to hackers.

Given the above and the time required to build effective barriers, digital security requires focused efforts to counter the malicious use of quantum computing, including the development and use of encryption techniques that are both "quantum-proof" and designed to work on "classical" computers.

- **Blockchain:** Blockchain, and other distributed ledger technologies (DLTs3), offer an alternative way of securing data and transaction records for use by multiple parties without reliance on a trusted, central authority. DLTs allow an immediate and secure digital transfer of value and ownership within a network, in total transparency through the tokenisation process where the right to a physical or digital asset are transferred into a digital representation – or token – on a blockchain. Being in possession of that digital token provides the right to that asset, and the ability to trade and track it digitally.

DLTs enable systems and the use of smart contracts allow ownership to be verified, confirmed and recorded in an automated, inimitable, transparent and near-instantaneous manner. The adoption of this technology in the transportation traffic sectors and in clearing and settlement processes offers significant efficiency gains and cost reductions. It will also lead to the disintermediation of many traditional financial and asset markets. While beneficial in many ways, blockchain technology raises a number of regulatory issues that range from payments, investments, taxes and accounting to compliance with anti-money laundering and combating the financing of terrorism policies, law enforcement and other crime prevention. Other policy implications of tokenised assets relate to international cooperation to limit regulatory arbitrage, the smooth operation of cross-border transactions, financial consumer protection, market integrity and financial education for the protection of investors in tokenised markets.

- **Metaverse:** Considered the backbone of the future entertainment economy, metaverse refers to a new generation of computing where instead of switching among discrete apps, people enter a collection of immersive digital worlds, which they explore in the form of cartoon avatars. Users will be able to do whatever they do in the physical world with a sense of presence that hasn’t been available online, thanks to three-dimensional designs they can experience through augmented – or virtual-reality headsets. Hence, the regulation of anti-social behavior on social media will take on additional dimensions. But that is not the only likely impact of metaverse. With its emergence and development linked to the rise of blockchain, crypto-currencies and non-fungible tokens (NFTs), the whole thing will allow users to do many things, including buy digital assets. As a result, the digital nature of assets in the metaverse, traditional legal concepts in lending, taking/providing contractual security, owning and selling assets, and enforcing security will likely require specific legal reforms to personal property security legislation to create additional legal and commercial certainties as legal issues in the digital asset space develop and modification of borrowing relationships between lender and borrowers.

When governments and technology companies consider our "digital" future, they should make Tim Berners-Lee's advice their lodestar: "Keeping the web open is not enough. We need to make sure that the web serves humanity and is used constructively, that it promotes truth and that it actually contributes to democracy." [25] This is a significant challenge to address.

The political philosophy that has underpinned the development of the internet and social media is libertarianism, which emphasizes the status of individuals as morally free persons and individual sovereignty, and asserts a strong distinction between the public and private spheres of life. No wonder social media has become a frenzy of narcissism!

The libertarian philosophy that permeates social media organizations is hardly reconcilable with a philosophy that privileges the common good. Democratic societies have no choice. The extreme danger posed by cyber threats to public and private organizations and to the fabric of societies demands that the

[25] Billy Perrigo, *The World Wide Web Turns 30 Today. Here's How Its Inventor Thinks We Can Fix It*, TIME, 12 March 2019.

philosophical divide be bridged in a way that sustains the common good while preserving the openness of the internet as a platform for well-being, innovation, and new sources of growth.

And as we enter the "AI era," this pursuit of the "common good" in cyberspace will need to be complemented by ethical guidelines and associated voluntary processes, technical standards, and codes of conduct aimed at ensuring that the unprecedented power unleashed by artificial intelligence improves humanity's chances of reaping the benefits of AI and avoids the risks that AI systems will not operate safely and securely.

Respect for human rights and democratic values are key ethical and equity concerns. For example, what limits should society place on the use of facial recognition tools? How can we best manage the risk of transferring bias from analog to digital works? Considerable effort is needed to conduct research on AI safety and to ensure that AI systems are transparent and accountable.