BRIEFING NOTES

BN-77-Emerging technology and military application-Aug2021

CYBERSECURITY, PRIVACY AND LIABILITY OF DIGITAL TECHNOLOGIES AND RELATED PUBLIC POLICY CHALLENGES

Authors: : Edward Gharibian[1] and Kash Khorasani[2]

1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

Vulnerabilities of Cybersecurity

- There are three factors affecting cybersecurity, namely (a) presence of criminal or state actors, (b) social, business and military dependency on IT technologies, and (c) vulnerabilities of IT systems and technologies that make them impossible to offer ideal secure solutions.
- Cybersecurity can be achieved, although not fully and completely, through the ***human, process and technology*** aspects.
- The weakest point of cyberneticist are humans themselves. Awareness of risk and adhesion to best practices can strengthen security of systems although often individuals either bypass security measures due to inconvenience or put too much of faith on technically insufficient security measures.

Human Factor

- The greatest vulnerability in any organization is the human resources themselves, indeed insiders are among the most common sources of cyberattacks to organizations' security.
- Many guidelines have been issued by governments and private sectors, aiming to educate and offer solutions to limit damages caused by insiders.

People Risk for Adapting New Technologies in Industry and Government

- The main problem for adoption of appropriate security measures in industries and governments, is lack of awareness and experts in the field. Emergence of smart manufacturing also known as Industry 4.0 systems and other Internet-of-Things (IoT) systems, that integrates traditional operational technologies (OT) with new IT technologies do indeed result in heterogeneous systems and environments.
- Engineers and staff who deploy solutions generally have knowledge of security either in IT technologies or Operational Technologies, and not on both.
- Emergence of Industry 4.0 and IoT related technologies in industrial units, introduces new technologies that are interconnected with existing and traditional ones, and thus people who work in such environments and that are familiar with OT need to learn and adapt themselves with new security measures.
- Military organizations and industries should empower and train employees by requiring security knowledge of Industry 4.0 and IoT before implementing them in their specific systems and units.
- Operational knowledge traditionally is concerned with optimal operation of units and via detection of faults and prevention of failure of units. However, now they

should also be trained to detect and prevent animalities due to cyberattacks and security violations.

Procedure

- *Military organizations need to define a proper set of rules and processes to effectively deal with cyber criminals and their changing strategies. US Government in an effort to make and standardize the cybersecurity procedures, has made recommendations through NIST cybersecurity framework.*
- *Canadian Government also has a set of recommendations for securing organizations, however not in the form of a set of standards.*
- *Other countries and European Union have also relevant non-mandatory documents and rules and procedures.*

Policy Challenge

- A key objective of rules and regulations is to raise awareness on individuals about their rights. These regulations need to be adapted by government stakeholders and businesses, however some do challenge to adjust themselves to new rules, where these rules in general generates more trust between military organizations and public stakeholders.
- Some of the most important barriers on implementing proper cybersecurity measures in military organizations and industrial units are as follows:

    - Balance between transparency and ethics versus procedures and policies is a challenging subject. Furthermore, improper security measures can be challenging for productivity of employees and CAF personnel.
    - Unwillingness to invest in security of companies and military organizations has been one of the main concerns.
    - Limited concerns to consider cybersecurity as a safety measure in government and industry to treat cybersecurity as a safety measure.
    - Lack of knowledge and technical capabilities in industrial and military systems.

- On the other hand, the most important challenges regarding public policy are:

    - There is no common definition and conflict of interests among the nations as a barrier for a global definition of cybersecurity and development of proper global policies

- *Cybersecurity is only one of the many significant public policy issues, and hence it may have conflict with other issues such as economic growth and liberty, which makes cybersecurity a challenging and crucial issue.*
- Liability issues should be addressed in national or international legislations and also per case law.
- *Rise of awareness of consumers of their rights based on the liability legislations.*

Introduction

Data is raw material for AI systems, and bigger data size, results in better decisions made by AI systems. Companies use these data to improve their products and services, that might threaten customers privacy. On the other hand, we are also surrounded by devices called IoT or smart things. Devices such as smart TVs, smart thermostats, smart refrigerators, smart cars, etc. These devices are practically internet connected sensors that collect our personal data. *With this amount of attention to data and AI, the privacy and liability of theses systems has become a real concern.*

However, it is not just our lifestyle that has evolved by emerging technologies, traditional factories and manufacturing units have started to adapt to new technologies and are connecting their equipment and systems to internet, a trend that is also supported by the Canadian Economic Strategy Table - Advanced Manufacturing [1], known as the Industry 4.0. In a nutshell, Industry 4.0 is a combination of IoT, cyber-physical systems (CPS) and the Internet of Systems [2].

Public Policy Shortcomings

Emerging technologies always create new issues on using private data, security and liability, that no one can fully anticipate ahead of time. This results in lack of proper law and regulation for new cases, that in turn challenge organizations for instance on how and to what extend collect the data, or concerns about investment in new technologies. It should also be noted that, all digital technologies and services in some manner, use internet as communication means and computer systems for storing and using data, that makes cybersecurity a priority.

Involvement of Internet and computer technology in everyday life, as well as different aspects of industry and organizations, make cybersecurity a major challenge for any

organization as well as public policy. Cybersecurity is not a pure technical subject. Internet is a means of improving security, prosperity and liberty of citizens, by providing open and reliable source of information, and limiting access to Internet technologies has always been a concern for human right activists and democratic nations [3]. This alone makes securing and governance of internet more challenging for policy makers.

Inherent cyberspace vulnerabilities and ever-growing number of criminal hackers as well as adversary states actors make security of digital assets a primary concern. This is due to the fact that many governmental organizations and agencies as well as critical infrastructures including electric grid, water supply networks, transportation systems, financial systems, etc. are relying on Internet technology. And with emergence of cloud computing, which is already widely in use and expects huge investments from large companies, the cybersecurity will be inevitable part of almost any type of service in the future.

Internet technologies have already been employed in more traditional manufacturing industries, and hence the cyber-criminals activities now can even result in physical damage. One should add to all of the above the ever-changing cyber-attack strategies, which adds another complication. For instance, in the wake of COVID-19 pandemic, there was a huge shift towards attacks with COVID-19 theme [4], or in another recent report it was revealed that cyberthreat targeting industrial entities has significantly increased [5].

Cybersecurity is a complicated subject, and its complexity is due to its interdisciplinary nature that needs knowledge and expertise in computer science, information technology, psychology, economics, organizational behavior, political science, engineering, sociology, international relations, and law to name some.

Cybersecurity challenges for public policy is not a new subject, and numerous bills have already been introduced, however governance of cyberspace have conflicts with other issues such as economic growth and liberty, that further complicates this subject for public policy [6].

But What is cybersecurity? Cybersecurity is the practice of protecting and defending computer systems, networks, data and software from attacks. Computer systems includes

servers, workstations, mobile devices, etc. that may or may not be connected to Internet. But apart from this technical definition, maybe the most acceptable formal definition of cybersecurity, by governments is what is defined in the Freedom Online Coalition [7]

> *"Cybersecurity is the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline". *as defined by ISO 27000 standard.*

At the time of writing of this report, Freedom Online Coalition is a partnership of 32 governments, mainly from Europe and North America. In this report, we will briefly introduce different threats and threat actors in the cyberspace and then will introduce the most important aspects of cybersecurity both for general cases and industrial units. We also will study existing data privacy rules and finally will go through some of the most important challenges that need solutions going forward.

Cyberthreat Landscape

The tactics and motivation of cyberspace attackers is continuously changing. In the past few years cryptomining has also been added to the major threat list. On the other hand, state sponsored hackers tend towards lower profile social engineering attacks. After COVID-19 outbreak a huge shift towards attacks that in some sort employ COVID-19 related themes have been reported all over the world.

Defense activities also see boosts, and many researchers are working in the field. Governments have published guidance for protecting small businesses and individuals against cyberthreat and specifically COVID-19 related scams. Training and education are still the best defensive approach. It is worth noting that cyberspace role on social and national security has been more emphasized with the recent political activities, and it would change in the current structure of cyberspace governance [8].

Main Sources of Cyberattacks

Cyber criminals take advantage of whatever circumstances they can, even the most unethical ones as in COVID-19, that at the time of writing this report already took more than four million lives and threatens several million more [9]. Attackers have been using COVID-19 theme in all types of attacks during the pandemic. On the other hand, increased

number of employees that are now working from home, and hence do not have the corporate level of protection offered by the Intrusion Protection Systems (IPS) and dedicated firewalls, make them more vulnerable to attacks. To better understand and manage cybersecurity risks, we will introduce the most important cyberattack sources.

- ***Malware*** is the most frequently used cyberthreat which accounts for about 30% of all data breaches in 2020 [10]. Malwares are also evolving and in recent years attacks move toward cryptojacking, however ransomwares are still a threat.

- ***Web based attacks*** use web systems and services to target the victims. The attackers use web browsers flaws or websites for attack. Malicious URL account for more than 80% of all attacks done on user's computers [11]. More than 275,000,000 unique malicious URL was reported in Q2 2020 [12]. For web applications, SQL attacks are the most frequent ones. However financial, retail and healthcare services which heavily rely on web base applications, potentially due to more investment in security has fewer vulnerabilities [8].
- ***Phishing*** mostly use email messages, that combined with some social engineering techniques, make the users to open a malicious attachment or click on an unsafe link. Phishing is the most important attack tactic that caused data breach with over 22% of all data breaches [10], and email phishing attacks is still the most important method of malware distribution [10]. The number of phishing attacks is growing, due to a huge amount of leaked personal data that helps attackers to produce more persuading messages. COVID-19 trigger a huge amount of phishing attacks via email, text messages and even phone calls [4], [13].

- ***(Distributed) Denial of Services*** is one of the highly impacted threats that has targeted almost any business [10]. Law enforcement have played a key role on fighting these attacks by taking down services like webstressor.org. On the other hand, increases of the number of connected devices and their dependency on IoT increases risk of nationwide DDoS attacks [8].

- ***Data breaches*** are the only topic that does not specifically apply to a threat but instead reflects a successful malicious attack. Healthcare and manufacturing sectors had highest number of data breaches. Insider share of data breaches in healthcare sector, has dropped from 23% in 2019 to 8.7 % in 2020, however it is not clear what

is the reason yet, and considering unusual working situation in 2020 due to COVID-19 pandemics, needs further studies. About 30% of breaches were caused by insider and about 25% caused by system error and glitches [10]. Canada leads in direct cost by 81 USD per compromised record and United States in indirect cost by 152 USD [8].

- ***Insider threat*** is a malicious threat comes from people within a company or organization that have inside information about data, computers, security practices, etc. Insider are considered current or former employee, contractor or partner who have information of the organization. Insider threat can be unintentionally by human error, for example due to by passing corporate protocols or intentionally. Many organizations employ protective mechanisms as intrusion protection systems (IPS) and firewalls, COVID-19 pandemic moved large number of workers from corporate offices to home, which practically put workers in less secure environments.
- ***Identity Theft*** is the theft of personal identification information. Considering that most of the personal information such as a bank account, home address, health records, etc. are stored in one's own devices or organization database, they are vulnerable to cyberattack.
- ***Cryptojacking*** also known as cryptomining is a new term that refers to a program that uses victim's device processing power to mine cryptocurrency.
- ***Ransomware*** attacks nowadays are evolving from stand-alone attacks to cyber-adversary. The victims of these attacks suffer from both financial losses and their credit. There has been a steady increase in the number of ransomwares incidences, such as the recent Wind River and the Colonial Pipeline attacks in US.

Threat Agents

Cybercriminals are the largest threat agents and their activities have been growing steadily. They are responsible for 80% of incidents [8]. They commonly use emails for their attacks. Email was involved in 90% of cyberattacks. Insiders are the second source of compromise by about 25% of incident in corporate environments. Nation sponsored and cyber-espionage are another important actors that were tried to increase the impact of attack by destroying critical infrastructure. Increased attacks in industrial control systems can be an indication of this attempt. Another trend in the state sponsored attack was increase attacks on banks. Hacktivists, cyberterrorist and script kiddies are other notable attack agents.

Vulnerabilities of Cybersecurity

There are three factor affecting cybersecurity, presence of criminal or state actors, social, business and military dependency on IT technologies, and vulnerabilities of IT systems and technologies that makes it impossible to offer a permanent solution [6].

Cybersecurity can be achieved, however not completely, through the ***human, process and technology*** aspects. The weakest point of cyberneticist are humans themselves. Awareness of risk and adhesion to best practice can strengthen the security of systems but often people either bypass security measures due to inconvenience or put too much of faith on technically insufficient security measures. And poorly designed technologies can result in both of these problems [6]. *Other factors as rapid technology development and innovation and changing nature of technology also affect security.*

Human Factor

The greatest vulnerability in any organization are the human resources themselves, indeed insiders are among the most common sources of attack to organization security. Insider risk is referred to any person who works in an organization that can cause threat to the confidentiality, integrity, and availability of the information inside the organization [14]. Insiders either intentionally or unintentionally may cause damage.

Insiders have both the knowledge and access to properties and can legitimately by pass security measures inside organizations and cause a substantial damage to assets. To prevent or minimize the risk of insiders, preparation and planning are required. However, keeping balance between fair and ethical treatment of employees and managing risks is a critical management task. Ethical approach to risk management requires transparent procedures and ethical policies.

Assets most vulnerable to insider attacks are confidential business information, credentials (username, password) of privileged accounts and sensitive personal information. The most dangerous groups of insider threat are employees, IT admins, contractors or temporary workers [8].

Many guidelines have been issued by governments or private sector, aiming to educated and offer solutions to limit damages by insiders. *These documents mainly emphasis on creating a cybersecure culture in an organization. The mindset is the critical component of culture of security in any organization and rising awareness inside the organization will lead*

to proper behaviour of individuals. The most important factor to influence awareness is leadership in organization, once leaders accepted the importance of cyber-security, the next step would be proper training of personals. Recognizing employee's behaviour and rewarding or punishment for that can have significant effects on the culture of security [15].

People Risk for Adapting New Technologies in Industry

The main problem for adoption of appropriate security measures in industry, is lack of awareness and experts in the field. Emergence of smart manufacturing also known as Industry 4.0 systems, combines traditional operational technologies (OT) with new IT technologies, resulting in a heterogeneous environment. The engineers and staff who deploy solutions generally have knowledge of security either in IT technologies or operational technologies, and not both of them. Smart manufacturing units, needs expertise of several area including, network security, embedded systems, OT and IT security, and with increasing number of these units, limited number of qualified experts become a serious concern and problem [16].

The emergence of Industry 4.0 related technologies in industrial units, introduces new technologies that are interconnected with existing traditional ones and thus people who work in such environments and are familiar with OT need to learn and adapt themselves with new security measures. Companies and industries should empower and train employees by required security knowledge of Industry 4.0 before implementing them in manufacturing units. Operational knowledge traditionally is concerned with optimal operation of units and via detection of faults and prevention of failure of units, now the should also be trained to detect and prevent animalities due to attacks and security violations. This need proper training and support by new technologies vendors and suppliers by introducing security aspects of their software and systems, upgrading operator's knowledge and skills. However, knowledge of securing legacy equipment should be taken seriously.

However, nowadays there is lack of proper and state of the art cybersecurity training for Industry 4.0, with proper and overall coverage of all required skills and knowledge [16]. A key subject here is to raise awareness on basic industrial control systems and secure methods for transferring them to Industry 4.0. Therefore, the people involved with security of Industry 4.0 should be trained with the latest required cybersecurity knowledge. It is also recommended to have relevant courses in schools and universities on Industry 4.0

security, for younger generation that in the long term will contribute to awareness of cybersecurity of cyber-physical systems [16].

Procedure

Organizations need to define a proper set of rules and processes to effectively deal with cyber criminals and their changing strategies. US government in an effort to make to standardize the cybersecurity procedures, recommendation use NIST cybersecurity framework [17]. Canadian government also has a set of recommendation [18] for securing organization however not in the form of standard. Other countries and European Union also have relevant non mandatory documents.

The following are the most important subjects that any organization need to follow in order to better protect themselves against cyberattacks. There are substantial amount of information and documents in this category, and here we will briefly present the essence for the Canadian government recommendations.

Holistic Insider Risk Management

Insiders have access to their organization resources and weather intentionally (i.e., maliciously) or unintentionally (i.e., negligence) can pose a high-risk and harm to their organizations. An effective management system should be developed and implemented policies for protecting both physical and cyber systems. The following are the most important approaches.

Culture of security. Organizations should develop strong policies and procedures for their physical assets as well as data and sensitive information handling inside the organization, with direct involvement of senior management. This, practically makes senior management responsible for the security of an organization. To develop an effective policy all relevant departments should be involved, also all levels of the company personnel must have a role in security of the organization.

Clear security policy and procedure is another vital part of the security, as annoyance of employees, partners or contractors for following procedure might lead to catastrophic damages. Any outsider (organization or individual) with access to the organization resources and data should be treated as risk. Identifying risks associated with the positions

and levels of employees in an organization is an important factor for managing risks, which can be identified by "periodic position assessments".

Manage third party and partners risk by including security measures in any agreement and understanding how key assets are physically located and structured. Hence, organizations first need to identify their critical assets and data, and then control or limit access of the contractors, partners, and consultants. Despite that security measures of the third-party providers are their own job, independent verification of them is recommended. Organizations should also maintain a long-term relationship with partners and key service providers.

Training and Getting to Know Employees

Employee screening at the hiring stage including social media activity of employee is advised. Moreover, a periodic (for instance every 5 years) or on promotions security checks are also required. Disabling accounts and preventing physical access of leaving employees is the responsibility of the management. Background checks must be done fairly and employees given the chance to dispute it.

Raising awareness on security and training is important since employees are "front-line of detecting and reporting potential insider risks". Employees should take continuously security awareness training to understand the risks specially regarding the use of social media and required security measures inside the company. People should be encouraged to report any unusual activity to the management.

Identify and Protect Key Asset

Organizations should identify and protect their key assets. Any asset that affects confidentiality, availability and integrity of their services should be categorized as a key asset. Key assets should be secured both physically and in cyberspace. This includes procedures for monitoring employee access to information and off-hour access to physical assets. Areas where physical access is restricted should be clearly identified with visual signs. And for information handling, minimum required access for an employee to handle her/his duties effectively should be assigned to them. Dividing key responsibilities among trusted personnel also reduces the risk of data misuse.

Monitor unusual behaviour along with effective employee awareness and care can help reduce insider attack. Specially, remote access of employees to sensitive data, should be restricted or at least monitored. Unusual incident or behaviour should be reported to the management and traced confidentially. Managers should take appropriate measures to minimize the risk associated with the incidents that are reported to them. Also, transparent policy for using social networks at the workplace should be developed and one makes sure employees are not posting sensitive data to social sites.

Protecting data by keeping an up-to-date backup is the first step on protecting against insider threat. Organizations should keep multiple copies of their data offsite, ensuring not any single person has access to both physical data medias and online data. Organizations should be aware of routs and methods that data can be accessed and exit out of organizations. Policies should be developed for downloading large amounts of data and accessing sensitive data.

Technology

Cybersecurity and its threats are dynamic due to the dynamic and changing nature of underlying technologies. Introduction of new technologies also adds to this complication as they do not completely replace previous technologies resulting in expansion of the attack surfaces and hence, new risks to the cyberspace.

Emergence of 5G/6G mobile communication technologies, which is the next generation of mobile networks is a good example. 5G/6G itself is much securer than current the LTE network, however based on the 3GPP roadmap [19] a stage in transition to 5G involves use of LTE network core, which will inherent all vulnerabilities of the LTE to the "5G non-standalone" network in first stage of implementation of 5G.
Somehow similar issues affecting the Industry 4.0, as new devices need to inter-operate with legacy equipment in a manufacturing unit, which most of them were designed when security was not a concern at all.

Legal Situation

Many nations have some sort of data protection and privacy rules for their citizens**.** Data protection is a central part of a democratic society and huge amount of personal and

business data are used in modern economies that require strong set of data protection rules for protecting personal and business data. Identity theft, leaks of sensitive data, and intrusive surveillance tools are some examples of these issues. Data protection has been a global issue and many countries have adopted certain regulations regarding data protection.

European parliament has passed some rules on personal data protection knows as General Data Protection Regulation (GDPR). In the past few years several companies have been fined in different European companies for violating theses rules [10]. Canada has some federal rules regarding privacy protection [11] and enforcement of these laws is handled by various governmental organizations. The data protection rules in Canada are governed by federal laws known as PIPEDA and three general private-sector laws in three provinces [11, 12] Canada also have anti-spam legislation. PIPEDA is a federal rule and applies to inter-province and international cases. The work of national courts and the Court of Justice of the European Union are also helping to create consistent interpretation of data protection rules.

Legal Issues

In the legal system, in order to be able to obtain a compensation for a physical or financial damage, one should be able to attribute fault to a party, through causation [6]. This is done either by breach of a contract terms or “breach of a duty of care in tort” [6]. A gap that is identified for most emerging technologies, is liability of technologies and the Issue is specifically complicated with AI technologies as the decision made in AI systems are more based on machine learning procedures and data provided to AI system and it is only loosely result of programming, which makes it difficult to tract a fault to a human error. This problem is known as “causation challenge” in law [6], [7].

The accountability of incidents is also unclear for smart manufacturing units, due to a number of stakeholders in supply chain, deciding on who is liable and the share of different stakeholders on incidents is challenging and unclear. Specially the longer lifespan of industrial products as compared to the IT products makes issues of liability more complicated for the industry sector. For Industry 4.0, the liability of technologies might be seen as a shared responsibility among developers, manufacturers, vendors, after sales services, among others.

European union Expert Group on liability and new technologies [8] in 2019 issued a report entitled “Liability for Artificial Intelligence and other emerging digital technologies” [9]. The report studied EU members law, and concluded that current regulation in many cases provide a basic protection for consumers of emerging theologies such as IoT, however in cases such as AI systems, that need analysis of complex structure and code of the system, the result can be unfair [9], [10].

Among the key findings in that report is that in cases that tort law fails, and providing evidence can be impossible or very expensive, existing legislation could not provide fair outcomes and new duty of care may need to be developed [9]-[11].

The office of Information and Privacy Commissioner (OIPC) of Canada, has proposed some enhancements to PIPEDA (The Personal Information Protection and Electronic Documents Act [12]) to address these challenges [13], [14].

The emerging technologies and AI are evolving and hence to protect the society and economy, politicians and legislators need a continuous flow of consumable information in order to make proper proposals and enhance the current regulations.

Overall considering the development and implementation of AI and other emerging technologies by large and multinational companies, the liability should be treated in both national and international legislation. Presently there are no clear and proper laws regarding the emerging technologies, therefore the most proper approach would seem to be identification of responsibility of stakeholders in the contracts. For consumer products, it is necessary to rise awareness of consumers through education and supply proper information about risks and their rights.

Policy Challenge

A key objective of rules and regulations is to raise awareness of individuals about their rights. These regulations need to be adapted by companies and businesses, however some companies challenge to adjust themselves to new rules, these rules in general generate more trust between businesses and customers.

The most important challenges in different aspects of cybersecurity can be summarized as follows.

Some of the most important barriers on implementing proper cybersecurity measures in businesses and industrial units are:

- Balance between transparency and ethics versus procedure and policy is a challenging subject. Moreover, improper security measures can be challenging for the productivity of employees.
- Unwillingness to invest in security in companies and manufacturing plants has been a concern.
- Limited concerns to consider cybersecurity as a safety measure in the industry to treat cybersecurity as a safety measure.
- Lack of knowledge and technical capabilities in industrial systems.

On the other hand, the most important challenges of the public policy are:

- There is no common definition, and also conflict of interests of nations is a barrier to a global definition of cybersecurity and development of proper global policies.
- Cybersecurity is only one of the many significant public policy issues, and hence it may have conflict with other issues as economic growth and liberty, which makes cybersecurity a challenge.
- Liability issue should be addressed in national or international legislation and also per case law.
- Rising awareness of consumers of their rights based on liability legislation.

Conclusion

Emerging technologies bring comfort to life and result in economic growth which eventually affect the prosperity of citizens, but the security and liability of these technologies also should be studied and grow with the same pace to prevent damages to both individuals and businesses.

Companies developing related technologies should do their best to offer secure products and as developers of technology they have the knowledge required to do so, however users and operators may not be in the same state/province. These make the training and exchange of knowledge one of the most important factors for securing the cyberspace and rising awareness of people. Transparency on personal data that are used by technologies is another important subject.

Despite the above users of technology which are humans are always prone to faults, either intentional or unintentional, and so proper policies and procedures should be implemented to protect organization assets and make both employees and companies liable for outcome of their actions.

In the point of view of public policy, prioritizing the subject of cybersecurity as well as developing new use cases in trot law are the most challenging subjects.

Also considering the complex nature of cybersecurity specifically for small businesses and individuals, educating and raising awareness of people are the most important subjects. Canadian government has several web sites and educational resources, but it is not likely to expect that most people will be able to use these sorts of resources, and hence adding these subjects to school and university curriculum might be a more practical approach.

The subject of cybersecurity and liability of emerging technology is a dynamic subject that with introduction of new technologies and new use cases change, and hence the governance of these technologies also need to be a dynamic and a continuous effort.

REFERENCES

[1] I. Government of Canada, "Report from Canada's Economic Strategy Tables: Advanced Manufacturing." https://www.ic.gc.ca/eic/site/098.nsf/eng/00021.html (accessed Oct. 13, 2020).

[2] "A critical look on Industry 4.0 | AllAboutLean.com," Dec. 29, 2015. https://www.allaboutlean.com/industry-4-0/ (accessed Oct. 13, 2020).

[3] "Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security," Dec. 21, 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx (accessed Oct. 13, 2020).

[4] "Landscape Update: Coronavirus Cyber Threats | Proofpoint US," Proofpoint, Mar. 18, 2020. https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update (accessed Oct. 12, 2020).

[5] Claroty, "Majority of Industrial Enterprises Face Increase in Cyber Threats Since COVID-19 Pandemic Began." https://www.prnewswire.com/news-releases/majority-of-industrial-enterprises-face-increase-in-cyber-threats-since-covid-19-pandemic-began-301145225.html (accessed Oct. 13, 2020).

[6] H. Porteous, "Cybersecurity: Technical and Policy Challenges," no. 2018, p. 24.

[7] "Why Do We Need a New Definition for Cybersecurity?," Freedom Online Coalition. https://freedomonlinecoalition.com/working-groups/working-group-1/blog8/ (accessed Oct. 13, 2020).

[8] European Union and Agency for Network and Information Security, ENISA threat landscape report 2018: 15 top cyberthreats and trends. 2019.

[9] "WHO Coronavirus Disease (COVID-19) Dashboard." https://covid19.who.int (accessed Oct. 13, 2020).

[10] "Verizon Data Breach Investigations Report 2020." https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (accessed Oct. 13, 2020).

[11] "Kaspersky Security Bulletin 2019. Statistics." https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf (accessed Oct. 12, 2020).

[12] "IT threat evolution Q2 2020. PC statistics." https://securelist.com/it-threat-evolution-q2-2020-pc-statistics/98292/ (accessed Oct. 12, 2020).

[13] N. B. · C. N. · P. Mar 19 and 2020 4:00 AM ET | Last Updated: March 19, "Here's what you need to know about the COVID-19 scams popping up in Canada | CBC News," CBC. https://www.cbc.ca/news/canada/toronto/coronavirus-scams-canada-1.5501958 (accessed Oct. 12, 2020).

[14] "CERT Insider Threat Center." https://resources.sei.cmu.edu/asset_files/Brochure/2017_015_001_452233.pdf (accessed Oct. 14, 2020).

[15] red3, "Cybersecurity is Everyone's Job," NIST, Oct. 15, 2018. https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job (accessed Oct. 14, 2020).

[16] "Industry 4.0 Cybersecurity: Challenges and Recommendations," May 2019. [Online]. Available: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

[17] nicole.keller@nist.gov, "Cybersecurity Framework," NIST, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Oct. 12, 2020).

[18] "Enhancing Canada's Critical Infrastructure Resilience to Insider Risk," Apr. 11, 2019. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx#a6 (accessed Jan. 15, 2020).

[19] "5G Security Issues." https://positive-tech.com/storage/5G-Research_A4.pdf (accessed Oct. 13, 2020.