BRIEFING NOTES

#BN-37-Cyber and space as key enablers-Feb2021

CYBERSECURITY 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

SUMMARY

- **Objectives:** Protecting the public security and prosperity should be the primary concern of any government. However, with existence of ubiquitous Internet, international criminals have also an almost instant access to most of the nation's resources and critical infrastructure. In order to make companies and individuals liable for the consequences of their actions, development of effective public policy directives and solutions is essential.
- **Scope:** Our investigations and studies have focused on the cyberspace including social media, encryption, among others and the threats that exist as well as the shortcomings of the current laws and regulations. Our investigations have led us to propose a number of recommendations on how to govern the cyberspace.
- **Target audiences:** Our investigated studies and research will provide and produce relevant and adequate material for public policy decision makers and will highlight the existing shortcomings in this domain and offer recommendations regarding the pitfalls of current legal situations for governance of the cyberspace.

CONTEXT

- Digital technologies such as AI, IoT, etc. have been increasingly employed in our every day's life as well as in industry. These devices and services rely on Internet to operate. On the other hand, inherited vulnerabilities associated with digital technologies and the growing number of cybercriminals as well as state sponsored hackers pose continuous threats to security of society and industry.
- Emerging technologies also result in novel methods for using data and new means to connect to Internet such as 5G technologies. This results in lack of proper laws and regulations for new cases, that in turn challenges organizations in investing in new technologies. It should also be noted that majority of digital technologies and services in one way or another use Internet as communication means and computer systems for storing and using data which makes cybersecurity a top national security priority.
- 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 the Internet technology, makes the cybersecurity a national security concern. With emergence of cloud computing, which is already widely in use and is witnessing significant investments from large companies [1], cybersecurity will be an inevitable part of almost any type of products and services in future.
- Internet is a tool for 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 [2]. This makes cybersecurity and governance of Internet more challenging for policy makers.
- Internet technologies have already been employed in more traditional manufacturing and critical infrastructure industries, and it is expected to grow in coming years [3].

Consequently, the cyber-criminal activities can now even target and result in physical damages.

- Criminals frequently change their attack strategies, which adds another complication for cybersecurity defences. For instance, in the wake of COVID-19 pandemic, there were significant shift towards attacks with COVID-19 theme [4]. A recent report revealed that cyberthreats targeting industrial entities have significantly increased after the COVID-19 outbreak [5].
- Cybersecurity is a complicated subject, and its complexity is due to its interdisciplinary nature, that needs knowledge and expertise from computer science, information technology, psychology, economics, organizational behavior, political science, engineering, sociology, international relations, and laws, to just name a few.
- There is no universally agreed upon standard definition for cybersecurity, and this makes cybersecurity challenging for public policy as it is not a new subject where numerous bills have already been introduced, however governance of cyberspace have conflicts with other concerns such as economic growth and liberty, that further complicates the subject for public policy decision makers [6].
- The most crucial challenge for both industry and the legal system is balance between human right and citizens security and power of government to extract encrypted data to track criminals and terrorists. Just recently US Department of Justice (DOJ), along with Canada, Japan, UK, India, Australia and New Zealand made an announcement [7], [8] for secure end-to-end encryption currently being used in many messaging systems, and called upon industries to offer solutions for governments to decrypt the messages under specific necessary situations.

CONSIDERATIONS

- Emerging digital technologies employing Internet and computer systems for communication and storing data. These systems are continuously being under attack by hackers where implementing proper cybersecurity procedures have become imperative and necessary to secure personal and business data and services.
- One of the biggest challenges of cyberspace is the free activity of cyber criminals, through fake social media accounts, phishing emails, malicious sites, just to name a few. Governance of social media while keeping a balance between the human rights and safety of the society is an urgent concern.
- Encryption technologies make the Internet more secure, but at the same time create a secure means of communication for criminals and terrorists that prove to be a challenge for governments.
- Different interpretation of the cybersecurity challenges in various countries has created a barrier for an international cooperation.
- Proper implementation of the cybersecurity procedures and protocols are further complicated and posses challenging issues for small companies, and are also not

mandatory, which may risk security and privacy of individuals that demand attention from the policy makers.

RECOMMENDATIONS

- To study and analyze current cybersecurity tools and best practices to determine shortcomings and subsequently propose investment opportunities for the government and military.
- To provide proper law enforcement and make companies that host fake or unsafe media and links, liable to their actions can hugely affect the cyberspace. These needs to be supported by continuous research to properly define and identify criminal actions in the cyberspace and offer proper remedies.
- In response to calls to Canadians and other governments for offering solutions for end-to-end encryption [7], universities and research centers also can investigate the legal burdens and support the development of technical-legal solutions.

REFERENCES

[1] L. Dignan, "IBM to spin off its managed infrastructure unit to focus on Red Hat, hybrid cloud; sees Q3 sales ahead of estimates," *ZDNet*. https://www.zdnet.com/article/ibm-to-spin-off-its-managed-infrastructure-unit-to-focus-on-red-hat-hybrid-cloud-sees-q3-sales-ahead-of-estimates/ (accessed Oct. 16, 2020).

[2] R. Goodale, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. 2018.

[3] 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).

[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] "International Statement: End-To-End Encryption and Public Safety," Oct. 11, 2020. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety (accessed Oct. 16, 2020).

[8] "US Department of Justice reignites the Battle to Break Encryption," *Naked Security*, Oct. 16, 2020. https://nakedsecurity.sophos.com/2020/10/16/us-department-of-justice-reignites-the-battle-to-break-encryption/ (accessed Oct. 16, 2020).

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