



# BRIEFING NOTES

#BN-17-Cyber and space as key enablers-Oct2020

## CYBERSECURITY AND PUBLIC POLICY

Authors: Rezvan Nozaripour<sup>1</sup> and Kash Khorasani<sup>2</sup>

<sup>1</sup> Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

<sup>2</sup> Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

## SUMMARY

- ✚ Prevention, detection and response are three essential consideration that we need to be concerned with in our cybersecurity strategy. Awareness of new threats, information sharing, better design, proper funding and timely reporting threats represent as some of the policies for addressing cybersecurity needs.
- ✚ Threat awareness is a first step facing adversaries in cyberspace. Hackers can use emerging technologies for generating new threats in cyber security. On the other hand, it is important to keep up with the latest technologies that will improve the cybersecurity.
- ✚ Cyber security professionals are obligated to follow certain ethical standards in all of these steps. Some of the most important ethical issues in cybersecurity are privacy, resource allocation, transparency and disclosure.
- ✚ Multiple policy approaches are available to minimize the number and significance of adversarial cyber operations and to enhance the cybersecurity.
- ✚ Awareness of new threats, information sharing, better design, proper funding and awareness of Cybercrime Public Reporting System represent as some these policies.

## CONTEXT

- ✚ With many frequent cyberattacks reported over the past few years, developing solid and concrete strategies is more important than ever. With that in mind, and treating trends in cyberattacks, it is essential to emphasize prevention, detection and response as the most important steps in your cyber security strategy.
- ✚ To address all of the above steps, it is important to consider some consideration in each step by minimizing the number and significance of adversarial cyber operations. Moreover, professional behaviors in this domain need to be ethical.
- ✚ A critical first step to face adversaries and act against cyber threats is awareness of new threats. In many cases, new technologies that have just hit the market are boons to hackers, who capitalize on people's lack of understanding of how those technologies work, as well as undiscovered vulnerabilities in new systems security.
- ✚ We need to emphasize the other emerging technologies that will improve the security of information systems from being attacked by hackers.

## CONSIDERATIONS

- ✚ **Ethical issues in cyber security:**
  - **Harms to Privacy:** Poor cybersecurity practices can reveal our lives and belongings, therefore they can be more than ineffective, they can be actually unethical.

- **Cybersecurity Resource Allocation:** cybersecurity efforts can negatively impact data storage capacity, network and download speeds, power efficiency, and system usability/reliability. Therefore, the role of finding a fair balance between resourceful cybersecurity and other functionalities is ethical.
- **Transparency and Disclosure:** Cybersecurity is a form of risk management, and it is an ethical obligation to report such risks when identified, so that informed decisions can be made by those capable and resourceful as well as concerned.

### **Cyber security challenges and issues:**

- **Awareness of New Threats:**
  - Information and communication technologies have been called as the fastest evolving technology space in human history, both in scale and properties. Many future security needs cannot be predicted and new and emerging properties further complicate the evolving threat environment.
  - Innovations such as quantum computing will undercut security of most online communications and data that are relying on encryption. Due to the significant processing capacity of quantum computers will unlock existing encryption keys that are based on computationally difficult-to-solve algorithms. This calls for the need of quantum-resistant solutions.
  - Researchers should be updated by new vulnerabilities that threaten a domain and find the best solutions to mitigate the effects of these threats. They should also be in consultation and collaboration with policy makers to inform them on the new areas of concern and press upon them to improve public policies to serve their security needs.
- **Information-sharing:**
  - First, one needs to promote information-sharing across organizations. When the government collects information that a cyberattack is under way, they need to immediately alert all other relevant and associated organizations and assess whether this could affect individuals or businesses. If it is found that cyberattacks could have a lasting effect the information must be diligently acted upon. Second, when security breaches are found with systems and servers, one needs to alert proper authorities to enhance the security software. Once this security software is enhanced, one needs to make it widely available to other government organizations and if appropriate, pass it on to suitable and appropriate individuals, organizations, and businesses. Information-sharing is probably the most important and effective step that one can take in preventing cyberattacks.
- **Better Design:**
  - Effective security needs to be an integral part of the design process. Developers have traditionally focused more on specifications,


requirements, and capabilities than security, for economic reasons. This make the design vulnerable to threats and attacks. Therefore, to better protect a domain it is recommended that designers and developers concerned about these vulnerabilities consider threats as a first step in their design to allow fewer opportunities for attackers to harm the system.

- **Proper Funding:**


- The federal government needs to provide cybersecurity the funding it needs and deserves. One needs to be developing the highest and most advanced levels of technology when it comes to securing key safety-critical infrastructure and computer systems and in order to accomplish that, ones needs to provide cybersecurity the proper funding it needs.

- **Awareness of Cybercrime Public Reporting System:**

- In Canada a new public reporting system for cybercrime was developed (The National Cybercrime Coordination Unit (NC3)). Any individual or business that has been the victim of or witness to a cybercrime will be able to use this system to report a cybercrime online.
- Although businesses and organizations may be aware of such a service offered by the government, individuals should also be made aware to report their incidents to this unit. Accordingly, governments should publicize existence of this unit. Therefore, an awareness through public relations firms and advertising campaigns should be seriously considered.

 **Emerging Technologies Posing a Cyber-threat:** Cybersecurity experts are highlighting certain technologies that have been repeatedly exploited by hackers, calling for greater understanding of their vulnerability to malicious actors. Some of these technologies are:

- Quantum computers
- 5G networks
- The Internet of Things (IoT)
- Artificial Intelligence (AI)
- Cloud Storage

 **Emerging Innovations in Technology that Will Improve Cyber Security:** It is important to keep up with the latest technologies as to not only stay up-to-date but safe, as well. We should be leveraging new technologies with the existing fundamentals that are in place to improve cyber security. Some of these technologies are:

- Hardware Authentication
- Cloud Technology
- Blockchain
- User-behavior analytics
- AI and Deep Learning