Security-Policy
NET
Nexus of
Emerging
Technologies

BRIEFING NOTES

#BN-44- Cyber and space as key enablers-Feb2021

GLOBAL COLLABORATION IS THE KEY TO EFFECTIVE CYBER DEFENSE

Authors: Rezvan Nozaripour[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

- The establishment of trust through agreed limits in the state-led cyberattacks and agreed ways to respond to cyberattacks (whether they are originated from states, commercial organizations, or criminal organizations) could be achieved realistically through increased international cooperation.
- There is a critical need for international policy alignment among allied governments to expose the adversarial and malicious cyber actors and establish norms for a global cyber protocols and behaviors.
- If there are no agreed upon and common agreements regarding appropriate levels of cyber operations by states, then cyberattacks may become even more common and could further escalate out of control.
- Increased international cooperation could also facilitate the development and implementation of appropriate technical measures to improve the cyber security of nations and in particular key safety-critical infrastructure.

CONTEXT

- The rapidly increasing of connected devices is causing significant growth in the cyberattack surfaces, making collaboration between organizations, governments and businesses more essential and important for eliminating system blind spots and for reducing losses.
- A combination of creative business level technologies and government level sound policy is required for effective cybersecurity to enable progress of the necessary technology and also to discourage bad actors. As cyber-threat players are involved across national boundaries, organizations and governments should collaborate to establish technical alliances and coordination within established global policies.
- Governments and global businesses need to establish strong cybersecurity technology partnerships to strengthen alignment of effective global cybersecurity policies to address today's threat landscape and to have better capabilities of competing with tomorrow's adversaries.

CONSIDERATIONS

- The integration of AI and edge-cloud processing will massively contribute to enhancing facial recognition technology and may be able to increase the public health security [2]. It may also result in an increased invasion of individual privacy concerns by these systems.
- These technologies will enhance deep learning in such a manner that it will provide access to faster and more broad set of data for training purposes. Therefore, the resulting AI systems become more capable and enhanced.

- Nevertheless, the problems and challenges with explainability of the AI systems still are prevalent [3].
- Challenges with adversaries where attackers may be able to access the wireless communication links between fog node and the edge device are considered quote serious. For example, an adversary accessing an edge-based facial recognition system would represent a great threat to the privacy and security of the citizens [4,5].

CONSIDERATIONS

- The first stage of collaboration should be between public and private sectors of global communities. They should work together to ensure that they get the basics right and to shore up the security of the internet for the good of all.
- The global community can secure the Internet through three collaborative events:
  - Internet service providers can apply system security measures by default, to ensure the correct routing of their Internet traffic. This could protect millions of customers.
  - Businesses can ensure that basic security measures are employed and mandate that their communication providers are also equipped with system security and software solutions.
  - Hardware providers also have a role to play in building system security to prevent attacks through hardware vulnerabilities.
- The next stage of this collaboration is outside of the borders and involves global collaboration between states. Industry and government have an obligation to act firmly on cyber security, in particular with the increasing and expanding threat landscape.
- Cybersecurity exceeds our traditional geographic lines. Bad actors do not take physical borders into account and therefore, our global strategy to struggle critical cybersecurity issues should not either.
- There is a need for global agreement in order to share best practices, learn about innovation strategies, and explore potential partnerships. Some of the key elements of this agreement can be envisaged follows:
  - There is a critical need for international policy alignment among allied governments to expose bad cyber actors and establish norms for cyber behavior.
  - Flexible, outcome-oriented cybersecurity policies can allow and raise the bar for improving cyber hygiene while allowing for continued innovation.
  - Effective public-private partnerships, including those with international allies, will be vital to helping protect critical national infrastructure.
- Global trade and economic interdependence create incentives for nation-states to come together and agree upon additional rules, or treaties, that collectively bind behavior and ensure the protection of shared resources.
- It is generally agreed that conventional laws apply online as well as offline, so certain types of cyber attacks are without any dispute regarded as illegal. However, additional agreements are needed regarding cyber operations. Specifically, if there is no common

agreement regarding appropriate level of cyber operations by states, then cyber attacks may become more common and could escalate out of control.

- Unless limits are internationally agreed upon, state-led cyber attacks threaten the trust required among stakeholders for effective internationally agreed cyber security goals, such as security of electronic commercial transactions and privacy of personal communications.
- The establishment of trust through agreed limits in state-led cyber attacks and agreed ways to respond to cyber attacks (whether originated from states, commercial organizations, or criminal organizations) could be achieved through increased international cooperation.
- Increased international cooperation could also facilitate development and implementation of appropriate technical measures to improve cyber security, which might include greater use of encryption and stronger encryption technologies.