Security-Policy NET
Nexus of Emerging Technologies

BRIEFING NOTES

# BN-20-Emerging technology and military application-Oct2020

PUBLIC POLICY AND ETHICAL ISSUES ON CYBERSECURITY AND SPACE ON DAILY LIFE

Authors: Shahram Shahkar[1], Paris Yazdjerdi[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

- Study the importance of cyber security, existing public policies and ethical issues
- Effects of emerging technologies on cyber security
- How to prevent a day without space and effect of a day without space on daily lifestyle and armed forces.
- Definition of dual use sciences and technologies.
- Dual use science and technology can represent as a potential threat to the public safety.
- Embedding ethics in future engineering and computing systems are essential to safeguard our nations against these potential threats.

CONTEXT

- **Public policy issues in cyber security**: Despite all the existing public policies covering various disciplines, the world of digital technologies and networking are being increasingly expanded in all aspects of our daily life. The main challenges are shortage in educated engineers and policy makers in this field.
- **Effects of emerging technology on cyber security**: Maintaining confidentiality and secrecy is becoming more challenging due to more advanced cyber-attacks using new technologies.
- **Prevention of a day without space to occur**: Dependence of societies on satellites and space is an obvious aspect of life nowadays which increases vulnerabilities of the space. Accordingly, it is very important to protect the security of space. Absence of space has negative impacts on our daily life but it impacts the armed forces as well which may lead to dangerous outcomes for a country.
- With the advent of the cyber world the prospects of public safety are rapidly changing. Terrorism is consistently and rapidly evolving towards deploying cyber space to counteract traditional measures that are set forth by governments to protect nations. Cyber threats and cyber-physical system threats require fewer financial resources, circumvent traditional surveillance protocols and mechanisms, and can be plotted with manageable human resources with far greater impact. Governments need to be vigilant and prepared for a robust and resilient line of defence as the society steps and immerses into the cyber space.

CONSIDERATIONS AND DISCUSSIONS

- Examples of dual-use technologies and threats they may pose to the public safety.
- Examples of some critical cyber physical systems and public safety dependencies on these systems.
- How feasible could it be to pose a nation-wide threat to public safety?
- How possible it is to fight back and what one can do to protect ourselves?

DISCUSSION

- Research based on current understandings can reasonably be anticipated to provide knowledge, products, and technologies that could be directly mis-applied by adversaries to pose threats to public health and safety. These technologies are referred to as “dual-use” research.
- Both researchers and public entities have roles and responsibilities in preventing mis-application of dual-use research and technology.
- Modern infrastructure extensively and increasingly relies on novel communication technologies and cyber space to deliver services to the public in a more reliable and economical fashion. Hydro-Quebec for instance is now relocating human forces more toward technical aspects of services as opposed to the administrative and logistics that can now rely more heavily on smart-meters, the cyber space and communication technologies.
- In spite of vast advantages that cyber-space and communication technologies are bringing to our societies, so are the associated threats and potential technological pandemics. For example, it can be theoretically shown that adversaries can break into electrical grids in a stealthy manner and orchestrate an avalanche of generator shut downs yielding vast persisting blackouts.
- If it could be possible to promote “ethics” in engineering systems (in addition to the nowadays “smart” systems), then every system would act according to certain ethical norms of societies. Especially when “autonomy” comes into play and a physical system independently decides based on its own senses of judgment, then one may expect a rationally explainable reaction from an ethical system in every (foreseen and unforeseen) circumstance.
- Some of the key questions that deserve further exploration are as follows. What is “ethics” and how it is possible to program ethics in a computerized process. What are the optimal set of rules that governments have to enact in order to ensure ethical behaviors from system technologists and designers?

FUTURE DIRECTION

In this study our goal was to outline the topics that are discussed above by refraining technical details and discuss the philosophical aspects encompassing future ethical systems that could inherently promote public safety, and be accepted and considered trustworthy to societies.