BRIEFING NOTES

#BN-50-Cyber and space as key enablers -Feb2021

DUAL USE SCIENCE AND TECHNOLOGY DEFINITIONS, ETHICS, AND CONCERNS

Authors: Shahram Shahkar[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

- 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

- 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 low 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

- Examples of dual-use technologies and threats they may pose to the public safety [2].
- Examples of some critical cyber physical systems and public safety dependencies on these systems [5].
- How feasible could it be to pose a nation-wide threat to public safety [6]?
- How possible it is to fight back and what one can do we 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 intelligent adversaries to pose threats to public health and safety. These technologies are referred to as “dual-use” research [5].
- Both researchers and public entities have roles and responsibilities in preventing mis-application of dual-use research and technology.
- Modern infrastructure is extensively and increasingly relying 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 the smart-meters, the cyber space and communication technologies [5].
- 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 [6].

- 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 [4].
- 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 behaviours from system technologists and designers [1],[4]?

CONCLUSION

- In this study our goal and aim were to outline and present the topics that are discussed above by presenting technical details and discuss the philosophical aspects that encompass future ethical systems that could inherently promote public safety, and be accepted and considered trustworthy to societies.

REFERENCES

[1] F. Alaieri, A. Vellino, Ethical Decision Making in Robots: Autonomy, Trust and Responsibility Autonomy, University of Ottawa.
[2] S. Tully, The Human Right to Access Electricity, The Electricity Journal Vol. 19, Pages 30-39, Issue 3, April 2006.
[3] Colin Allen,Iva Smit, Wendell Wallach, Artificial Morality:Top-Down, Bottom-Up, and Hybrid Approaches. Ethics and Information Technology, 7(3):149-155, 2005.
[4] Gordana Dodig Crnkovic, Daniel Persson, Sharing Moral Responsibility with Robots: A Pragmatic Approach. Tenth Scandinavian Conference on Artificial Intelligence: SCAI 2008, pages 165-168, 2008.
[5] Cyber Science & Technology at the Army Research Laboratory (ARL), Journal of Cyber Security and Information Systems, Volume: 5 Number: 1.
[6] Ethically Aligned Design, IEEE Advancing Technology for Humanity, First Edition, 2019.