QUICK IMPACT

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

AUGUST 8, 2020

Governing the Future(s) of Emerging Technologies in Canada[1]

Kristen Csenkey
NAADSN Graduate Fellow and PhD Candidate at the Balsillie School of International Affairs

Dr. Nina Bindel
Postdoctoral Fellow at the Institute for Quantum Computing (IQC) at the University of Waterloo

Introduction

Emerging technologies are new innovations that can cause disruptive change in society. They can disrupt the old ways of doing things and knowing about the world. Artificial Intelligence (AI), quantum computing, the Internet of Things (IoT), and the fifth generation of telecommunications infrastructure (5G) are examples of emerging technologies.

There are risks associated with emerging technologies, especially those with military applications. Canada's National Defence Policy, *Strong, Secure, Engaged*, sees the use and management of emerging technologies as a defence and security issue. Adversarial actors can use these technologies to develop a competitive edge and engage in threatening behaviour more efficiently.

Risks, 'Gridlock', and Pathways of Governance

There are three ways to think about the risks related to emerging technologies and their impacts on Canadian society: 1) national sovereignty of innovation, 2) threats to critical infrastructure (CI), and 3) data and network security.

The intersection of emerging technologies and the governance of their associated risks is blocked by 'gridlock'. This 'gridlock' is a self-reinforcing cycle of interdependence between institutions where solutions to problems

are difficult to achieve. Combined with the disruptive nature of emerging technologies, the problem of gridlock can become amplified. Thus, Canada needs to take measures to effectively navigate the governance of emerging technologies, including both the associated risks and opportunities. While there is no single or correct solution to managing these issues, there are some options for moving beyond the problem and towards a solution.

There are seven 'pathways' to move beyond the governance gridlock:

1) Shifts in the interests of major power players can help reduce gridlock by managing global problems. This means that a state could champion an issue area and lead the way in addressing the associated challenges.
2) Autonomous and adaptive international institutions can modify their mandates to reflect developing challenges more quickly by creating new rules and pathways through the gridlock.
3) Technical groups with effective and legitimate processes can help push through the issues preventing effective governance because they can adapt quickly to change and are generally removed from state-to-state politics.
4) Diverse organizations and institutions can work together to help entrench common norms and goals in policy. Although fragmentation caused by differences in goals between institutions and states can cause gridlock, adding or expanding on existing norms may help move the process along.
5) Mobilization for cooperation and compliance calls for domestic actors and organizations to work towards changing norms and practices at an international level.
6) Civil society coalitions can organize and gain support for certain initiatives when they partner with other organizations and states. This pathway is guided by social movements that are headed by civil society groups and the cause is championed by states.
7) Innovative leadership entails recognizing the ineffectiveness of the current governance structures and then developing new strategies or structures that help address the problem. New actors are 'norm entrepreneurs' who use their agency to define values and goals and then implement them.

We see a role for Canada in these pathways in the governance of emerging technologies through ensuring IT-security even in the presence of quantum computers.

Increased Cooperation in Standard Setting: Quantum-Safe Cryptography

Large-scale quantum computers promise to enable computations that are otherwise too inefficient for current computers. However, these advances also pose a threat: using large-scale quantum computers will make it possible to break essentially all public-key cryptography in-use today, such as RSA public-key encryption (PKE) or digital signature schemes. Given the importance of IT-security ensured by cryptographic algorithms, this would have a serious impact on the safety and economic well-being of ordinary people as well as companies and governments.

To prepare for this security threat, cryptographers have been working on alternative algorithms which are not known to be vulnerable to quantum attacks—the so-called post-quantum or quantum-secure cryptographic algorithms. In order to advance this effort, in 2017 the US-American National Institute of Standards and

Technology (NIST) launched a new standardization process with the goal of selecting the next generation of quantum-secure public-key cryptographic algorithms. According to the current schedule, the final standards will be available in 2022/2024.

Indisputably the outcome of NIST's post-quantum standardization effort will impact the decisions of other standardization agencies worldwide. In particular, close partners of the U.S, such as Canada, will likely favor the same algorithms. This is particularly reasonable in this case as researchers recommend a transition to post-quantum cryptography sooner rather than later and running a sovereign standardization takes time and is costly. However, no standardization agency should blindly follow the decision of another country[2]. NIST's post-quantum standardization effort, however, seems to be trustworthy for the following reasons:

- It is community-based, which increases the chance to detect weaknesses.
- The background of submitters of cryptographic algorithms is diverse with a mix of international researchers from academia and industry, decreasing the risk of national interests and increasing the chance to foresee different kinds of risks.
- NIST allows a rather large degree of flexibility in that changes to the submissions are encouraged in order to improve the algorithms.

Another important property to ensure trust in a standardization process is transparency. In particular, it should be made transparent

1. why a particular candidate was preferred over another one to avoid non-scientific selection biases, and
2. what the difference between the submitted and standardized algorithms are and why they were introduced to avoid, e.g., backdoors or implementation mistakes.

As also urged by other Canadian researchers, an advisory board to monitor and evaluate NIST's post-quantum standardization effort to decide whether to follow NIST's recommendations should be formed, corresponding to the above-mentioned pathway three to move beyond gridlock. The decision about the trustworthiness should, in particular, be based on the degree of transparency of the final decisions as discussed above.

If NIST's standardization process is evaluated as being trustworthy, the standards should also be adapted as Canadian standards and post-quantum security should be required for cryptographic-based security systems that protect data for medium- and long-term information lifespan, corresponding to pathway five.

In addition, non-government CIs of which a lack of security pose great risk, such as in the financial market, logistics, or power plants should be identified and a mandatory risk assessment of these CIs should be implemented. Similarly, and based on the developed recommendations and standards, the risk posed by quantum computers and how to mitigate it, should be communicated to small and large businesses and the general public, corresponding to the sixth pathway to move beyond gridlock.

This way, Canada can benefit from the advances of international partners to transition to quantum-safe cryptography in a fast and secure way.

Conclusion

In sum, the risks associated with emerging technologies can be managed through multiple and overlapping pathways. Managing these technologies is as important as developing effective governance frameworks. Without effective governance, the problem of gridlock will remain. The bottom line is that governance of these challenges needs to be more transparent, flexible, restructured to facilitate cooperation. New forms of cooperation should foster transparency about the risks of emerging technologies, communicate policy alternatives, and define and enforce responsibilities.

---

[1] This *Quick Impact* is a modified version of a publication supported by the Department of National Defence Mobilizing Insights in Defence and Security (MINDS) Targeted Engagement Grant, which appeared originally in Kristen Csenkey (ed.) "*Simplifying Emerging Technologies: Risks and How to Mitigate Them*", Balsillie School of International Affairs, May 2020. https://www.naadsn.ca/wp-content/uploads/2020/07/Simplifying-Emerging-Technologies.pdf

[2] For example, in 2015 a backdoor in NIST's standard of a pseudo-random generator has been revealed, raising distrust for other NIST standards as well.