
# BRIEFING NOTES

# BN-27-The role of AI-Oct2020

## THE RISE OF INDUSTRIAL CYBER DEFENCE POWER IN THE 21ST CENTURY – REGULATION AND PUBLIC PARTNERSHIPS

Authors: Dave McMahon
Clairvoyance Cyber Corp (www.clairvoyance.network)
info@clairvoyance.network (819.664.2708)

Industry is innovating at a pace that governments cannot match nor will they every be able to in the foreseeable future. Cyber power yielded by the private sector has exceeded that of nation states including that ability to defend forward through persistent engagement with pacing threats. The CAF will need to partner with and invest in, a strong and sovereign cyber defence industrial base in order to compete with adversaries and remain relevant on the global stage.

Governance poses significant challenges in a rapidly globalizing world. In the emerging future, governments will need to grapple with a new world order in which power diffuses among corporations, empowered individuals, civil society, criminal organizations, and peer and near-peer nation-states. The power-shift will be particularly acute in the cyber domain[1] and will precipitate a re-adjustment of Westphalia models towards a new construct.

Telecommunications companies and Technology giants such as Microsoft, Facebook, Google and Amazon have become new world superpowers.[2] Each of these platforms has more clients then most countries have citizens and a revenue to match a nation's GNP. We have known for quite some time, that the interdependencies between Canadians and industrial infrastructure is measurably more critical.[3]

The "Internet and digital technologies [have] change[d] deeply the economics of regulation and more generally the economics of institutional frameworks."[4]

"The 20th century tools we have for protecting a free society won't work for 21st century giants. Each country including Canada has to set up safeguards. That's the grand experiment that we are living with. The thing is, we don't know what the right balance of regulation versus economic enablement is. The scale and speed of the big tech companies, which constitute FAANG (Facebook, Apple, Amazon, Netflix, and Google) plus Microsoft, are going beyond what regulators can keep up with. Regulators move too slowly, and the tech giants are one or two steps ahead. Telecommunications companies, content delivery providers and tech giants are not evil. They are simply forcing us to rethink what the digital ethics of the 21st century should be. The answer is you have to learn how to be flexible."[5] Disruptive technologies like AI have outpaced disciplines such as ethics and philosophy.

[1] Cyberspace is owned, operated and controlled by the private sector.
[2] The 20th century tools we have for protecting a free society won't work for 21st century giants - Tony Wong - Toronto Star, July 22, 2019
[3] Study Interdependencies between critical infrastructures- Public Safety, Bell Canada, RAND Corp 2005
[4] Multilevel Governance of the Digital Space. - Eric Brousseau, University of Paris X, Institut Universitaire de France, EconomiX, 27/07/05
5 Brian Hopkins, vice-president and principal analyst of U.S.-based consulting firm and think tank Forrester Research

For centuries, territory has been by marked by borders, governed by sovereign states and the rule-of-law. Yet, cyberspace is global, and borderless. It is owned and operated by the private sector and defined by its digital natives. The circumstance of disruptive technology, globalization, multi-level Internet governance and polycentrism[6] break traditional domains-of-control, and entangle private, public, domestic and international levels-of-authority.

The centre-of-authority for cyberspace has migrated. It is less about imperial power and more about multinational corporations, non-government organizations, philanthropy, and social agency. "This trend toward Internet sovereignty is complicating efforts at enhancing cybersecurity and clarifying governance."[7]

The principle of state regulation is no longer relevant because the problems they addressed change with the new technologies.

"Facebook announced recently that it is looking at launching its own cryptocurrency called Libra, which is both "brilliant" and dangerous at the same time. It's a brilliant move because they already have such a big reach but now they would be in charge of a system that will turn them into a bank with responsibility for potentially billions of dollars worth of payments. Look at the requirements and scrutiny that banks have to go through. We would have to rethink the rules once again."[8]

"I think it's easy for us to villainize these companies, but ultimately I believe they are good for us. Money is certainly at stake, but most of these companies have a socially progressive west coast ethic, and at some level aren't purely corporate profiteers. But they are certainly pushing the bounds of digital ethics and the notions of what is public and what is private. And that's what we have to figure out: How do we let them innovate but without surrendering the rights we hold dear?"[9]

[Meanwhile] Canada and other western democracies are being leapfrogged by former developing countries as the new technologies are being implemented.[10] The CAF needs a comprehensive strategy that addresses the integration of 5G, IoT, Cloud, and Quantum computing.

Cyber is a domain where the interests, values, norms and strategy of the Western liberal democratic vision of open networks and Internet freedom, is countered by alternative models posed by states

[6] Polycentrism is the principle of organization of a region around several political, social, financial centres or cyber domains.
[7] Robert K. Knake, Council on Foreign Relations, Internet Governance in an Age of Cyber Insecurity 3 (2010)
[8] Forrester Research
[9] Forrester Research
[10] Forrester Research

seeking to restrict and control the Internet along nationalistic boundaries. These "multipolar politics and the prevailing status quo of strategic ambiguity hinder international cyber regulation."[11]

The Realpolitik of cyber power is not just about regulatory governance framework. In the evolution of state and civilian cyber power the "oscillation in the balance of power may be peaking, but never before could a dozen people in their pyjamas meaningfully annul the monopoly on the use of force."[12] There are cyber capabilities now wielded by the private sector for which there is no analog by nation-states.

The future will see the continued diffusion of power and influence from nation-states to non-traditional actors, particularly in cyberspace, and the disintermediation of governments in this space. Cyber has shifted the power-balance and will remain strategically significant for the foreseeable future.

"In reality, Canada has no choice but to let the [owner-operators of cyberspace] self-regulate since government doesn't have the tools to work at their scale and speed."[13]

Equitable and trusted industrial partnerships will be critical should CAF wish to remain relevant in Cyberspace.

[11] Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished? https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf
[12] Chapter 5 – State power and cyber power, 2018 Security Outlook Potential Risks and Threats – Canadian Security Intelligence Service
[13] Forrester Research