BRIEFING NOTES

# BN-2-COVID19-June2020

RE-DEFINING CYBER POWER - POST COVID-19

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

INTRODUCTION

As part of the Department of National Defence and Canadian Armed Forces' (DND/CAF) response to COVID-19, the Mobilizing Insights in Defence and Security (MINDS) program has invited collaborative networks to help the Defence Team analyze, understand, and learn from the pandemic. The Goal of Academic Outreach is to inject external observations, assessments, and recommendations into DND/CAF in order to improve policy development, decision making, and subject matter expertise.

BACKGROUND - SHIFT HAPPENS

Cyber will be the most significant catalyst for change in the future and will be at the centre of acute transformation within the military. COVID-19 has accelerated that change.

"*The next natural disaster of pandemic will trigger violent digital transformation, the result of which is that everything will be mediated by cyber technology. Meanwhile, our adversaries will choose this time to strike western democracies with cyber exploitation, misinformation campaigns of chaos while criminally capitalizing on the events and purposefully interfering within critical infrastructure sectors including: healthcare, emergency services, industry and defence. The capability of organizations to operate outside of the conventional office, adapt business processes, adopt next generation secure cyber technology and recalibrate to the new reality, will be put to the test*."[1]

CONSIDERATIONS

- **GLOBAL CONTEXT**

  Changing demographics, resource competition, environmental stresses, globalization, economics, governance, urbanization, geopolitics, shifting power and the unprecedented advancement in science and technology are significant trends sharing the future security environment and every organization. This monoculture of singular tends can be forecast with a measure of certainly towards 2040. However, the emergent effect of convergent trends, technologies with black swan events such as pandemics and politics, will be more dramatic. Emergent effects that are derived from physical, human and cyber domains, now represent new risks to CAF; ones which are opaque to conventional military doctrine.[2]

  The contest to control and influence the fabric of cyberspace will be as significant as the Manhattan project and the space race. China and Russia represent pacing threats to Canada. Technologies like fifth generation mobile communications (5G), artificial intelligence (AI),

[1] Clairvoyance Cyber Corp, Cyber Defence Foresighting Initiative, 2018

[2] Future Security Environment 2040, Clairvoyance Cyber Corp for the Canadian Armed Forces

Quantum Computing, Big Data and the Internet-of-Everything (IoE) represent the vital high-ground. Bytes are as core to the business as bullets and battleships.

MILITARY IMPLICATIONS

We are fighting a land, sea, air and space battle in the information domain. Cyber power is doubling every year, and the adversarial innovation cycle can be measured in weeks. Technology will drive: doctrinal change, operational plans, advanced cyber warrior training, mission assurance, platform and infrastructure protection.

This COVID-19 event is unlike a conventional natural disaster, when the military is called upon by the civil authority to deliver purely physical assistance. This time is different. National security and defence may require the military to counter foreign influence and disinformation, conduct active cyber defence during a time of intensified cyber attacks and provide more nuanced support to critical infrastructures under threat. Sectors such as: healthcare, safety, telecommunications, finance and the defence industrial base.

"State-sponsored actors likely are using the COVID-19 pandemic climate to dig for important intelligence, including how COVID-19 is affecting military preparedness," warns a bulletin from Communications Security Establishment.

The Canadian-led NATO battle group in Latvia has already been the target of a pandemic-related disinformation campaign as well as sophisticated cyber attacks originating from Russia. Canadian Security Intelligence Service, have been warning that threat actors likely will target organizations doing COVID-19-related research in order to steal intellectual property linked to the pandemic.

All the while, the CAF is undergoing its own dramatic digital transformation, adjusting to adaptive dispersed operations on a new terrain, and an rapidly expanding attack surface, while relying on civilian command control communications infrastructure whilst forming new partnerships with civil defence forces.

Competition, conflict and war between states is occurring on cyber terrain owned, operated and controlled by entities other than the CAF. COVID-19 has shown this acutely. The cyber security industry has detected an order-of-magnitude more attacks from nation-state actors against Canada, while circumventing direct military/security/law enforcement confrontation. Cyber is core to space platforms, ships will behave as floating data centres, aircraft will look like software in the cloud, and soldier systems act as fog computing. Fifth generation mobile communications (5G) will connect everything-everywhere, all the time. Post COVID-19, remote communications over public infrastructure and personal devices is the new normal.

Mega cities will be the most densely sensored environments on the planet - with 1 million devices per square km. A handful of these devices will have more bandwidth than the entire Internet connectivity of the CAF today.

COVOD-19 has triggered dramatic digital transformation, the result of which is that everything is now curated by cyber technology. Overnight, the network has been pushed out of central control to the edge (onto personal mobile phones) up into the cloud (collaborative tools) - off corporate infrastructure.

Secure remote mobile cellular communications will be the defining technology for the CAF, while personal mobile devices will remain highly-susceptible to exploitation.[3]

Our adversaries have invested heavily in dominating this technology[4]. It is likely that 5G will be deployed sooner than the full operational capability of major cyber programmes in the CAF. Thus, the CAF mission set may need to quickly re-calibrate for an Everything-on-5G World, where China is the most dominant global super-power.

Cyber power can only be understood in a global context.

SHIFT IN CYBER POWER

Governance poses significant challenges in a rapidly globalizing world. In the emerging future, governments must 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. Instability will likely spread rapidly as oscillations in power and public sentiment become more common and as borders become less relevant. The power-shift will be particularly acute in the cyber domain and will precipitate a re-adjustment of Westphalian models to a new construct.

Militaries, if they are unable to adapt and respond to power-shifts accelerated by digital empowerment, will find themselves overcome by non-state actors usurping national control. A few sophisticated individuals with access to the power of the cloud can effectively challenge Canadian defences[5].

[3] https://www.blackberry.com/us/en/products/resource-center/2020-threat-report/mobile-security
https://www.wandera.com/mobile-threat-landscape/
https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf

[4] China's Belt and Road initiative

[5] The Hactivist group Anonymous successfully crippled the Canadian Federal Government for several weeks with a DDoS Attack. Confirmed today that Government of Canada GC servers have been cyber attacked. Until full service is restored please use 1-800-OCanada. — Tony Clement (@TonyclementCPC) June 17, 2015

Today, our world is principally described by data, and subject to global influence at the speed-of-light. The sudden reliance on personal mobile communications by the public sector and military represents instability and risk where rapid technological convergence has created a frictionless state between the human terrain, the network and the Internet-of-Things (IoT). Open media, big-data, ubiquitous mobile communications and the IoT are at the centre of identity, security, defence and privacy issues facing us today. Yet, in many countries around the world, open access to the Internet is Balkanized, blocked, censored, shaped, controlled and denied. Norms and legal framework struggle to keep pace with rate of change, or have failed completely. Platform providers, not governments will define cyber norms and laws.

Technological advancements could empower military leaders to engage adversaries with minimal overt involvement and precisely where the engagement results in the most favorable outcome. The covert action conducted in the cyber domain will be the 'invisible hand' that influences populations, markets, geopolitics, and military balance of power. Commanders may favor soft-power non-kinetic capabilities (cyber and influence) as alternate approaches to conflict resolution.

Conflict in cyberspace is asymmetric, unrestricted and irregular. Situational understanding and maneuver warfare in this domain will be vital for military and political advantage. Strategic listening and targeting will be tightly coupled across domains. Axiological targeting particularly in cyber space will become even more complex within the context of deterrence, escalation or retaliation. Cyber provides high-tech warfare at knife-point range.

On top of the inherent complexities and uncertainties involved in the cyber domain, a shared international framework of cyber deterrence would have to bridge cultural divides, force and network structures, national strategies and objectives, national and commercial level decision-making processes as well as concepts of proportionality. Attribution is likely the hardest problem for cyber but is also the most necessary for effective deterrence, active cyber defence and will be required by law.[6]

FINDINGS

The CAF will likely find themselves involved in a hybrid, irregular, and asymmetric conflict fought on cyber terrain they neither own or control. In this future, leading with soft power, cyber and influence may be the preferred options. Strategic deterrence will need a credible active cyber defence capability in which to project power and influence globally and throughout Cyberspace in the defence of Canada.

[6] Cyber Attribution of Sophisticated Threat Actors in the Defence of Canada, 2020, by R9B, SapperLabs and Clairvoyance Cyber Corp for Canadian Armed Forces

There is no going back from the digital transformation precipitated by COVID-19. A good deal of military cyber infrastructure is critically dependent upon personal mobile communications, the Internet, public cloud and applications. Strong industrial partnerships will be essential to enable both defensive and offensive cyber operations.

Defining success and victory in the future will become increasingly difficult, but what is certain is that cyber will be at the core. An assessment of principal patterns and technology trends will provide a foundation and the examination of the character of future conflict provides a context for developing several credible views of the future.

NEXT STEPS (If applicable)

Continued anticipatory intelligence, strategic foresighting, applied experimentation, modelling and simulation will be necessary to mitigate future risks beyond COVID-19. Purposeful investment in cyber defence science and technology innovation and industrial partnerships, will be required to keep pace rapidly evolving cyber mission and build a sovereign capability.[7]

[7] There have been limited cyber capabilities deployed since 2010. Cyber defence programs conceived nearly a decade ago are scheduled for delivery 2024-2026. There are no programs planned past that date. Current capability deficit is estimated at 20 years. Expedited procurement of industrial capability and rapid innovation is required to close the gap with allies and adversaries.