Canadian Global Affairs Institute
Institut canadien des affaires mondiales

Lessons from COVID-19 for 5G and Internet Security

by Randolph Mank

April 2020

POLICY PERSPECTIVE

LESSONS FROM COVID-19 FOR 5G AND INTERNET SECURITY

by Randolph Mank

CGAI Fellow

April 2020

Canadian Global Affairs Institute
Institut canadien des affaires mondiales

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

ISBN: 978-1-77397-125-4

The deadly COVID-19 pandemic has pushed all other issues to the back burner of public discourse in Canada and internationally. Yet the debate over 5G, and China's corporate role in it through the Huawei corporation, was a hot button issue prior to the pandemic. Its importance has in no way diminished.

In fact, the emerging idea that the world should move to even greater reliance on the digital economy makes internet and web security even more important.[1] As we sift through the coming nationalist-fuelled debates over repatriating critical supply lines and decision-making, we need to recognize that the web and the internet must remain world-wide and secure.

If so, with China's credibility damaged over the early denials of the lethality of the virus, can Western nations trust its official assurances on 5G neutrality? Are we prepared for the worst if the fears about 5G became a reality?

The answers go well beyond Huawei and 5G to the international system for ensuring internet security.

Where are we in the 5G debate?

Before COVID-19, the issue of whether or not to allow China's Huawei corporation to provide the fifth generation (5G) of internet equipment in Canada and other Western countries was hotly contested in public forums.[2] China's rise as the potential usurper of American power and ideological challenger to the liberal international order makes the matter fundamental in the context of escalating superpower competition.

The main practical advantages of 5G internet access – dramatically increased speed and capacity – make its adoption inevitable. The issue is whether to allow a Chinese company with the cheapest and readiest equipment to gain the contracts, or to favour smaller competitors such as Ericsson and Nokia, despite their handicaps of cost and scale.[3]

Two distinguishing features of 5G technology are the need for many more small aerials and the greater use of software for more efficient use of the available broadband spectrum. The main fear is that Huawei, a company closely associated with the Chinese government and military, along with the Communist Party that runs both, will design a backdoor in the software or hardware that allows it to hack or plant viruses in the system at will, with potentially fatal security consequences

[1] Though sometimes used interchangeably, the internet is the physical infrastructure consisting of connected computers and undersea cables, while the World Wide Web is the network of information that sits within it. https://www.geeksforgeeks.org/whats-difference-internet-web/

[2] J. Longo, "5G Raises Tough Policy Choices for Canada," Johnson Shoyama Graduate School of Public Policy, Aug. 13, 2019. https://www.schoolofpublicpolicy.sk.ca/research/publications/policy-brief/5G-raises-tough-policy-choices-for-Canada.php

[3] T. Wheeler, "5G in Five (not so) Easy Pieces," Brookings Institution, July 9, 2019. https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/

for the digital economy and critical infrastructure.[4] Though fears may be exaggerated, a 5G system designed and operated by Huawei could give China a significant strategic advantage in future.

Cyber-security is already a problem with existing technology. Moreover, since China already tightly controls the internet within its own borders – blocking Western social networking platforms while using them to manipulate opinions and systems in the West – skepticism about their commitment to a free and open internet globally is warranted. If China doesn't trust Facebook, Twitter and other U.S. corporations to operate within its borders for security reasons, it's fair to ask why any Western country would trust Huawei to have such a vital role in engineering their 5G systems.

The 5G debate in Canada was already adrift before the pandemic. Telecommunications corporations had been using Huawei equipment to varying degrees and offering 5G-ready devices to customers.[5] Huawei is also well entrenched through advertising and research funding across the country.[6]

Yet the U.S. has taken steps to block Huawei from its own networks and indicated that its Five Eyes intelligence-sharing partners should follow suit.[7] Among those partners, the United Kingdom has taken what could be a tentative decision to grant limited access to Huawei, believing it can ring-fence 5G systems to eliminate vulnerabilities. Australia and New Zealand have taken firmer stands against using Huawei equipment, leaving Canada as the only partner yet to decide.

Canada's position is complicated by the ongoing house arrest of Huawei's CFO in Vancouver on an extradition request from the U.S., and China's retaliatory imprisonment of two Canadians, along with other punitive measures.[8] A negative decision on Huawei's role in 5G could further imperil the Canadian detainees, who are already being held in oppressive conditions.

Thus, Canada remains stuck in deciding about Huawei's role in 5G deployment. Artful delay can be a useful tactic in diplomacy. Unfortunately, the lessons of the pandemic suggest that delay can also have extremely dangerous consequences if security risks are left unmitigated.

[4] C. Perez, "5G Explained – Part Three: National Security," *Foreign Policy*, March 31, 2020. https://foreignpolicy.com/2020/03/31/5g-cellular-huawei-china-networks-national-security-power-map/

[5] S. Clark, "The WhistleOut 5G Wireless Guide for Canada (2020)," *WhistleOut*, March 25, 2020. https://www.whistleout.ca/CellPhones/Guides/5g-in-canada-wireless

[6] T. Blackwell, "Canadian Governments Give Huawei Millions in Funding While Debate Rages Over its 5G Role," *National Post*, Feb. 3, 2020. https://nationalpost.com/news/canadian-governments-give-huawei-millions-in-funding-while-debate-rages-over-its-5g-role

[7] R. L. Strayer, "US Policy on 5G Technology," Foreign Press Center Briefing, New York, NY, Aug. 28, 2019. https://www.state.gov/US-Policy-On-5g-Technology

[8] D. DaSilva, "Huawei CFO Awaits Court Ruling on US Extradition Request," *Financial Times*, Jan. 23, 2020. https://www.ft.com/content/bc26950a-3e1c-11ea-a01a-bae547046735

What lessons can be learned from the COVID-19 crisis?

Once the pandemic crisis has passed, governments everywhere will no doubt launch lessons-learned inquiries.[9] Leaving aside the medical dimensions, we can already see the need for much better crisis planning and preparation, nationally and globally.

But an even more pertinent lesson is also clear: every aspect of daily life during the pandemic has relied on the internet, including the delivery of government support and services, global and national communications, business continuity, critical infrastructure and even entertainment. Moreover, responses to every other global issue rely on a fully functioning and secure internet. In short, without a fully functioning internet the pandemic crisis would have been immeasurably worse.

This brings us back to the core issue at stake in the 5G debate. Neither the global system, nor any of its nations individually, can risk the possibility that the internet or the web could be disrupted, either deliberately or accidentally. And, as much as information security itself is of paramount importance in the rollout of 5G, the possibility that the growing Internet of Things itself could be weaponized or destabilized is even more critical.[10]

In summary, as with pandemics, we need to have effective plans in place to detect and deal with any future internet crisis, be prepared to execute those plans quickly should a crisis occur, and have credible international institutions to co-ordinate a global response.

But there is a fundamental problem. While the techniques for dealing with pandemics have been well known for centuries, handling large-scale internet disruption still represents untrodden ground.

What national decisions are needed now?

Deciding whether or not to permit Huawei to participate in the 5G rollout in Canada poses difficult choices. If the answer is no, then commitments already made will need to be reversed, which will be expensive. Relations with China will deteriorate even further, jeopardizing the safety of Canadians, and likely resulting in additional punitive trade measures and more hostile relations in general.

As bad as that would be, if the Canadian government were to green-light Huawei, the repercussions could be even more detrimental, as defence and intelligence officials have warned.[11] Relations with the U.S., upon which Canada's prosperity and security largely depend, would be

[9] L. Freedman, "How the World Health Organisation's Failure to Challenge China over Coronavirus Cost us Dearly," *New Statesman,* April 5, 2020. https://www.newstatesman.com/world/asia/2020/04/how-world-health-organisation-s-failure-challenge-china-over-coronavirus-cost-us

[10] L. Gorman, "5G is Where China and the West Finally Diverge," *The Atlantic,* Jan. 5, 2020. https://www.theatlantic.com/ideas/archive/2020/01/5g-where-china-and-west-finally-diverge/604309/

[11] L. Berthiaume, "Military Concerned about Chinese Access to Networks as Huawei Decision Looms," *The Globe and Mail,"* March 12, 2020. https://www.theglobeandmail.com/canada/article-military-concerned-about-chinese-access-to-networks-as-huawei-decision-2/

dealt a significant blow. Intelligence sharing would be curtailed. Daily cross-border communications, both civilian and military, could also be hampered.

The Canadian government has a plan to mitigate cyber-risks, but it has not been widely tested inside government, or with the public.[12] Alternative fail-safe means of communicating and maintaining functioning public systems would need to be created. Stockpiling of essential supplies would need to be comprehensive.

The problem is that the collective human imagination bends toward discounting such extreme scenarios in the face of the enormous effort required to prevent them. Moreover, even in the unlikely event that Canada or any other country alone could succeed in defending against such a black swan event, it would still be dependent on an unprepared and inadequate international system.

Could there be a better way forward on a more global basis?

Pursuing cyber-deterrence: A MAD, MAD world

In the inevitable post-COVID-19 triage on globalization, superpower decoupling will not be a realistic option when it comes to managing the internet. And, of course, the superpowers aren't the only players in cyber-space. As a result, the answers to the 5G dilemma go beyond any one country or corporation to the global system for governing the internet itself.

While there is no shortage of discussion groups on cyber-security within the UN, NATO and other global forums, it remains unclear which international institutions would actually be empowered to deal with such a crisis.[13] If the U.S. has repudiated the World Health Organization for its handling of the pandemic, the likelihood that the U.S. would assign such authority for managing the internet to the UN's International Telecommunications Union (ITU) would be even more remote. Indeed, the U.S., the EU and Canada have been consistently opposed to such a role for the ITU.[14]

Instead, the International Corporation for Assigned Names and Numbers (ICANN) – the little-known umbrella organization for an array of internet management groups that work to maintain the internet's operation – is the preferred bottom-up multi-stakeholder model, in keeping with the original idea of a free and open internet.[15] However, these institutions are not designed to manage global conflict involving the internet.

[12] Public Safety Canada, "National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age," 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

[13] Though Canada is not a contributor, the NATO Cooperative Cyber Defence Centre of Excellence does interesting work in the field and is a useful source of information on activities underway internationally. See https://ccdcoe.org/

[14] M. O'Reilly, "Reining in the UN's Little Known International Telecommunications Union," *The Hill*, Aug. 8, 2018. https://thehill.com/opinion/technology/400990-reigning-in-uns-little-known-international-telecommunication-union

[15] Centre for International Governance Innovation and the Royal Institute of

If neither the ITU nor the ICANN network is fit for purpose, then we're on risky ground. What appears to be missing is a central organizing principle for maintaining internet security.

For this, perhaps we could take cues from another technological output of the Quantum Age; namely, nuclear technology. It came to be understood during the Cold War that, despite all the national preparedness planning against nuclear attacks, the only real path to peaceful coexistence was through the principle of deterrence.

Nuclear deterrence has been successfully organized around the principle known somewhat perversely as *mutually assured destruction* (MAD). Though now repudiated by some (particularly those who prefer missile defence systems),[16] it is this principle that deters the use of nuclear weapons to this day. If one country were to launch a nuclear attack, it could be assured of equal or greater retaliation.

As much as we would prefer a world with perfect defensive shields, the reality is that we need a similar organizing principle for deterring major cyber-attacks. Call it mutually assured disruption. If one hostile nation were to launch an overt or covert cyber-attack on another, or on the physical apparatus of the internet itself in a target area – a widely anticipated element of modern conflict – it must be assured of an equally disruptive response.

Of course, malicious non-state actors also threaten cyber-security. Better co-ordinated international institutions could also help detect and take collective action against grey zone cyber-attacks by organized crime, terrorists and other actors.

If we were to organize around such a deterrence principle, it would accelerate the need, not only for building national offensive cyber-capacities as is now underway in Canada and elsewhere,[17] but also for creating international architecture to detect and deter cyber-attacks. As with nuclear, this would include bilateral and multilateral agreements between the superpowers, containing confidence-building measures as well as regional and international organizations for monitoring and control.

Unless and until we are prepared to pursue cyber-deterrence, any decision that allows one country to gain a technological advantage over others in access to and control of the internet will have a destabilizing effect on both national and international security.

Conclusions

Far from being inconsequential, the rollout of 5G is a decision that should be taken in the interests of national and global security, more than expediency and cost. While it is necessary for Canada

International Affairs, "Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance," 2016. https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf

[16] R. Jervis, "The Dustbin of History: Mutual Assured Destruction," *Foreign Policy*, Nov. 9, 2009. https://foreignpolicy.com/2009/11/09/the-dustbin-of-history-mutual-assured-destruction/

[17] Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy*, Section 6, 2017.

and other Western countries to impose a pause on Huawei, it is insufficient to assume that internet security will flow from that decision.

As with pandemics, threats to the internet are already known and very real. As dependency on the internet increases, its security requires serious worst-case planning, though planning can never be fail-safe. Internet security will also require credible global governance and institutions based on sound principles of deterrence.

As inimical as it sounds, a MAD, MAD global architecture may be the best hope for ensuring future global security.

About the Author

Randolph Mank *is a three-time Canadian ambassador and former VP of BlackBerry. He currently heads MankGlobal Inc. consulting, and serves as a Fellow of the Canadian Global Affairs Institute and the Balsillie School of International Affairs.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.