POLICY Brief

JOHNSON SHOYAMA
GRADUATE SCHOOL OF PUBLIC POLICY
UREGINA USASK

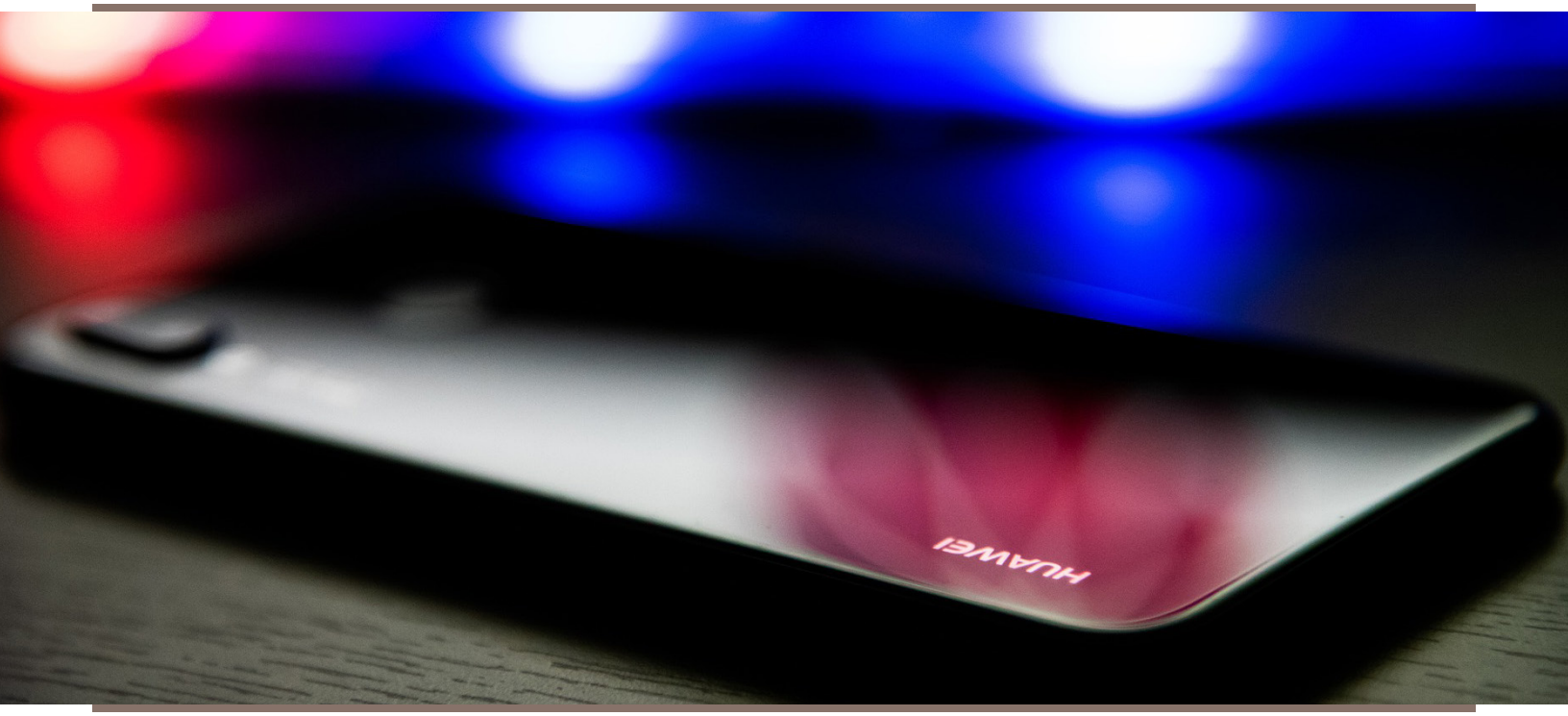

PHOTO CREDIT: FARUKGARIB14 FROM PIXABAY

Beyond Huawei: The Urgency of Digital Security

David Sparling, Master of Public Policy student, Johnson Shoyama Graduate School of Public Policy

June 15, 2020

Over the past decade, cybersecurity has emerged as a crucial dimension of Canada's national security policymaking. Its importance will only increase as Canada completes the transition to fifth generation (5G) telecommunications infrastructure. Despite popular conspiracy theories tying 5G technology to the COVID-19 pandemic and secret government plots, the scientific and economic consensus is clear that the transition to 5G is crucial to the future of Canada's digital economy and related advances, including machine learning, Internet of Things (IoT), and artificial intelligence (AI). The evolution of Canada's telecommunications networks requires a substantial increase in the number of cellular sites to realize the promise of faster downloads and an enhanced web of telecoms coverage. This digital infrastructure project would be accelerated through the participation of Chinese megacorporation Huawei, an international telecoms leader that provides equipment at much cheaper rates than competitors such as Ericsson and Nokia.

However, Huawei has been consistently labeled as an arm of the Chinese Communist Party by the United States. As a member of the Five Eyes network, the influential intelligence-sharing consortium made up of the United States, the United Kingdom, Australia, and New Zealand, Canada has faced both internal and external pressures to exclude Huawei from commercial 5G networks on national security grounds, most notably from the administration of U.S. President Donald Trump. White House officials have repeatedly stated that Canada's future participation in the Five Eyes alliance would be imperiled by Huawei's inclusion. It has been a far-reaching campaign against Huawei, with the Trump administration pressuring more than 60 countries to follow its lead on Huawei. Still only a handful of nations have complied. But the calculation for Canada is in many respects qualitatively different from other nations. Compared to other American allies, such as India or South Korea, Canada's national security apparatus is uniquely integrated with and dependent upon the United States. Complicating this dilemma further is Beijing's belligerent protection of Huawei's commercial interests and its willingness to engage in hostage diplomacy and export restrictions against Canada, as demonstrated by the arrests of Canadians Michael Kovrig and Michael Spavor following the arrest of Huawei CFO Meng Wanzhou in December 2018. Adding to this complexity, Huawei enjoys support from major Canadian telecoms provider Bell, as well as academic institutions such as the University of British Columbia and the University of Regina, which have partnered with Huawei on tens of millions of dollars worth of 5G research.

However, the tide of Canadian public opinion may be turning on Huawei. A May 13, 2020 poll conducted by the Angus Reid Institute revealed that 80 per cent of Canadians felt that the federal government should bar Huawei from participation in the construction of the country's 5G networks. Moreover, on June 3, 2020 Montreal-based telecom provider BCE announced that it would be relying on Swedish equipment supplier Ericsson to build the critical antennas and base stations for its 5G network. In a separate announcement, Telus stated it had chosen Ericsson and Finland-based supplier Nokia to support the construction of its 5G radio access network equipment. This announcement signals a substantial about-face on the part of Telus, which had stated in February 2020 that it intended to bring its 5G networks online using Huawei gear by the end of the year. In January 2020, Rogers was the first major telecom provider in Canada to activate its 5G network using Ericsson equipment. Roger's competitors BCE and Telus have now followed suit by rejecting Huawei equipment.

The sudden shift in support away from working with Huawei within the Canadian telecoms industry may help resolve the issue by default on the practical grounds that the major private telecoms have made their corporate choice, spurring the federal government on to a decision barring Huawei. To preserve the intelligence sharing and security cooperation facilitated through the Five Eyes network, the federal government should heed the advice of CSIS officials, Five Eyes allies, corporate stakeholders, and the Canadian public and ban Huawei. Although this move would undoubtedly provoke further economic and political retribution from Beijing, preventing the possibility of 5G-enabled cyberattacks is an overriding security priority. Ottawa cannot erase the current animosity in Sino-Canadian relations by succumbing to the will of the People's Republic of China on 5G. The bottom line is that next-generation digital infrastructure is simply too important to Canada's future prosperity and security for anything less than decisive action on this file.

"The bottom line is that next-generation digital infrastructure is simply too important to Canada's future prosperity and security for anything less than decisive action on this file."

The Division Within

Canada's intelligence community remains deeply divided on the Huawei issue, pending the results of a still-ongoing federal security review into 5G. Canadian Security Intelligence Services (CSIS) officials consistently portray Beijing as a purveyor of cyber-threats facilitated through Chinese corporations, with Huawei a prime example. Although the opinions and testimony of former intelligence officials need not be taken as representative of the current institutional paradigm of CSIS, a similarly wary characterization is described in China in the Age of Strategic Rivalry, the synthesized conclusions of a 2018 CSIS research workshop. CSIS officials have also drawn attention to China's 2017 National Intelligence Law, which requires China-based corporations such as Huawei to cooperate with intelligence services, as well as persistent concerns over backdoor hardware vulnerabilities in Huawei equipment. In the hands of skilled hackers, these vulnerabilities could lead to wide-scale data theft or even the disruption of infrastructure and services that rely on 5G, making digital infrastructure integrity a serious national security threat. Moreover, these risks ensure that the inclusion of Huawei in the 5G networks of Canada and the United Kingdom could undermine the intelligence sharing processes at the core of the longstanding Five Eyes agreement.

In contrast to the wariness over Chinese digital influences demonstrated by past and present CSIS representatives, the Communications Security Establishment (CSE) has more often downplayed the geopolitical dynamics of the 5G security debate. Instead, CSE head Scott Jones has presented Canadian security screening processes as detached from global politics and as more effective than those of Canada's allies in the Five Eyes. During a September 22, 2018 sitting of the Standing House Committee on Public Safety and National Security, Jones testified that any security vulnerabilities associated with the use of Huawei gear would be identified and mitigated by existing screening processes. Jones' position placed his organization at odds with the conclusions of CSIS and Five Eyes intelligence allies, particularly those of American and Australian security officials. As repeatedly emphasized by American lawmakers, Ottawa's heterodoxy over the role of Chinese firms in digital infrastructure construction represents a challenge for Canada's current intelligence-sharing framework.

The varying perspectives on Chinese cybersecurity threats presented by Canada's two key intelligence agencies represent a policy challenge in the context of relationships with both China and Five Eyes allies, particularly the United States. This division within the Canadian intelligence community is a continuation of a lengthy Canadian tradition of internal government disagreements over how to conceptualize and conduct the Sino-Canadian relationship.

Complex cybersecurity concerns associated with 5G and other emerging technologies lend an additional layer of complexity and controversy to an already fraught bilateral relationship. As the Government of Canada attempts to reconstitute Sino-Canadian relations, the increasingly crucial digital dimension of this relationship must be navigated through a careful, whole-of-government approach that incorporates the perspectives of both CSE and CSIS, while modernizing national security frameworks to safeguard core infrastructure.

"As repeatedly emphasized by American lawmakers, Ottawa's heterodoxy over the role of Chinese firms in digital infrastructure construction represents a challenge for Canada's current intelligence-sharing framework."

The Way Forward

Regardless of the outcome and consequences of the Huawei decision, protecting Canadian digital infrastructure from cyberthreats will remain a national security imperative for the foreseeable future. The federal government should take quick action in this critical field.

- To safeguard Canada's digital economy from both state and nonstate cyber threats, the Government of Canada should develop a Digital Infrastructure Integrity Strategy. The country needs a nationwide, systemic framework for identifying, responding to, and countering threats to Canada's 5G network and related technologies, including the Internet of Things (digitally connected machines) and Artificial Intelligence (digital "thinking" machines). The strategy would require close cooperation between the federal security apparatus and partners in Canadian universities, the telecommunications sector, and provincial and territorial governments. This approach would produce a robust range of policy measures that would improve the cyber resilience of Canada's core internet infrastructure. It would constitute a much-needed step towards modernizing Canada's national security frameworks, safeguarding Canadians' data, and improving defences against malign digital influences.
- Given the centrality of the Five Eyes intelligence network in shaping Canadian cybersecurity policy, the Government of Canada should also propose the creation of a dedicated, transparent forum for assessing and developing strategies for contemporary cybersecurity threats in partnership with security allies. The creation of such a forum among the Five Eyes nations and other close intelligence allies such as France, Germany, Japan, South Korea and India would strengthen intelligence-sharing processes and reduce Canada's security dependence upon the United States. Disunity between Five Eyes member nations have been on full display in public debates over Huawei and 5G. Informed by this experience, the creation of a new international forum between democratic intelligence allies would mitigate divisiveness and boost coordination on future cybersecurity issues.

Critics might argue that the creation of such a forum would undermine the sovereign decision-making processes of member nations. In the face of heightened cybersecurity vulnerabilities and rapidly developing technological challenges, however, enhanced cybersecurity cooperation between Canada and its allies should be both strengthened and encouraged. A formalized process of intergovernmental and inter-agency cooperation on cyber-threats and technological security would allow an expanded Five Eyes network to streamline intelligence-sharing while mitigating risks of damaging international relations between participant states. Nor must the creation of this forum herald a formal return to Cold War geopolitics. On the contrary, the development of formalized norms governing state cyber-conduct among the Five Eyes nations could provide a foundation for broader conversations between the United States, Russia, China, and other major powers. One outcome could be the emergence of an international code of conduct for cyberoperations. Admittedly a more likely outcome would be entrenching geopolitical divisions in the digital sphere as China and Russia seek to challenge the hegemony of the United States and its allies. In this eventuality, however, greater cooperation between Canada and like-minded allies would be more important to cybersecurity policy than ever.

"The country [Canada] needs a nationwide, systemic framework for identifying, responding to, and countering threats to Canada's 5G network and related technologies, including the Internet of Things (digitally connected machines) and Artificial Intelligence (digital "thinking" machines)."

As a middle power with a finite amount of international clout, Ottawa has a limited ability to initiate either the creation of the proposed forum or broader multilateral negotiations. Having said that, since the 1945 San Francisco conference that produced the post-Second World War international system, Canada has occasionally played an outsized role in mobilizing the international community. Taking the lead on promoting a rules-based order for state cyber conduct could represent a return to this diplomatic tradition. By proposing the creation of this forum, the federal government could stimulate international conversations on policy solutions for bridging the divide between techno-nationalism and techno-internationalism. University of British Columbia scholar Paul Evans describes these phenomena as "the securitization of technological development", whereby sensitive and emerging technologies such as 5G, artificial intelligence, and data science are reconceived as integral planks of national power and security.

Although it is highly unlikely that China would accept an international cyber-regime based on western norms without significant concessions, it is nonetheless desirable for the Government of Canada to encourage an international consensus on the rules of cyber-conduct. In recent years, the PRC has employed revisionist tactics that often flout agreed-upon rules and norms, as displayed through Beijing's relentless bullying of Canada following the December 2018 arrest of Huawei CFO Meng Wanzhou. However, even a pragmatic understanding of current Chinese conduct emphasizes the desirability of a rules-based digital order. It is within the interests of Chinese state to establish a clearly delineated framework governing the permissible actions of state actors in the digital realm to safeguard its own economy from external attack. Although strained Sino-Canadian relations may hinder Ottawa's ability to play the role of interlocutor between China and the United States on digital cooperation, the federal government should nonetheless support the establishment of a stable international order for conducting cyberoperations.

PHOTO CREDIT: S. HERMANN & F. RICHTER FROM PIXABAY

Considering the growing importance of 5G, AI, big data, and other techno-nationalist policy areas to contemporary geopolitics, working towards an authoritative international framework for digital conduct may be necessary to avoid international cyberwarfare on an unprecedented scale.

References

Visit www.schoolofpublicpolicy.sk.ca for a complete list of references.

ISSN 2369-0224 (Print) ISSN 2369-0232 (Online)

David Sparling

David Sparling is a Master of Public Policy student at the Johnson Shoyama Graduate School of Public Policy's University of Saskatchewan (USask) campus. A lifelong Saskatchewan resident, David completed a Bachelor of Arts (Honours) majoring in Political Studies at the U of S in June 2018, graduating with high honours. David's master's thesis, "Cybersecurity at a Crossroads: Sino-Canadian Relations in a Digital Context" was funded by the Social Sciences and Humanities Research Council (SSHRC) and the Department of National Defence's Mobilizing Insights in National Defence initiative (MINDS). David's research applies qualitative content analysis to the debates of Canada's Parliament to clarify issues related to the intersection of Canada-China relations and cybersecurity. David has a passion for knowledge and a love of storytelling and creative writing, as well as a keen interest in Canada-Asia relationships.

People who are passionate about public policy know that the Province of Saskatchewan has pioneered some of Canada's major policy innovations. The two distinguished public servants after whom the school is named, Albert W. Johnson and Thomas K. Shoyama, used their practical and theoretical knowledge to challenge existing policies and practices, as well as to explore new policies and organizational forms. Earning the label, "the Greatest Generation," they and their colleagues became part of a group of modernizers who saw government as a positive catalyst of change in post-war Canada. They created a legacy of achievement in public administration and professionalism in public service that remains a continuing inspiration for public servants in Saskatchewan and across the country. The Johnson Shoyama Graduate School of Public Policy is proud to carry on the tradition by educating students interested in and devoted to advancing public value.

For more information on the Johnson Shoyama Graduate School, visit www.schoolofpublicpolicy.sk.ca