UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Special Committee on Canada-China Relations

Submission by
Dr. Christopher Parsons
Senior Research Associate
Citizen Lab, Munk School of Global Affairs & Public Policy
University of Toronto

Introduction

1. I am a senior research associate at the Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto. My research explores the intersection of law, policy, and technology, and focuses on issues of national security, data security, and data privacy. I submit these comments in a professional capacity representing my views and those of the Citizen Lab.

Background

2. Successive international efforts to globalize trade and supply chains have led to many products being designed, developed, manufactured, or shipped through China. This has, in part, meant that Chinese companies are regularly involved in the creation and distribution of products that are used in the daily lives of billions of people around the world, including products that are integrated into Canadians' personal lives and the critical infrastructures on which they depend. The Chinese government's increasing assertiveness on the international stage and its belligerent behaviours, in tandem with opaque national security laws, have led to questioning in many Western countries of the extent to which products which come from China can be trusted. In particular, two questions are regularly raised: might supply chains be used as diplomatic or trade leverage or, alternately, will products produced in, transited through, or operated from China be used to facilitate government intelligence, attack, or influence operations?
3. For decades there have been constant concerns about managing technology products' supply chains.[1] In recent years, they have focused on telecommunications equipment, such as that produced by ZTE and Huawei,[2] as well as the ways that social media platforms such as WeChat or TikTok could be surreptitiously used to advance the Chinese government's interests. As a result of these concerns some of Canada's allies have formally or informally blocked Chinese telecommunications vendors' equipment from critical infrastructure. In the United States, military personnel are restricted in which mobile devices they can buy on base and they are advised to not use applications like TikTok, and the Trump administration aggressively sought to modify the terms under which Chinese social media platforms were available in the United States marketplace.
4. Legislators and some security professionals have worried that ZTE or Huawei products might be deliberately modified to facilitate Chinese intelligence or attack operations, or be drawn into bilateral negotiations or conflicts that could arise with the Chinese government. Further, social media platforms might be used to facilitate surveillance of international users of the

[1] See: Clair Brown and Greg Linden. (2005). "Offshoring in the Semiconductor Industry: A Historical Perspective," at: http://isapapers.pitt.edu/58/1/2005-02_Brown.pdf.

[2] The Citizen Lab has published a comprehensive report on Huawei and 5G, and the Canadian equities at play. Many comments in this submission are derived from that research. See: https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/.

applications, or the platforms' algorithms could be configured to censor content or to conduct imperceptible influence operations.

5. Just as there are generalized concerns about supply chains there are also profound worries about the state of computer (in)security. Serious computer vulnerabilities are exposed and exploited on a daily basis. State operators take advantage of vulnerabilities in hardware and software alike to facilitate computer network discovery, exploitation, and attack operations, with operations often divided between formal national security organs, branches of national militaries, and informal state-adjacent (and often criminal) operators. Criminal organizations, similarly, discover and take advantage of vulnerabilities in digital systems to conduct identity theft, steal intellectual property for clients or to sell on black markets, use and monetize vulnerabilities in ransomware campaigns, and otherwise engage in socially deleterious activities.
6. In aggregate, issues of supply chain management and computer insecurity raise baseline questions of trust: how can we trust that equipment or platforms have not been deliberately modified or exploited to the detriment of Canadian interests? And given the state of computer insecurity, how can we rely on technologies with distributed and international development and production teams? In the rest of this submission, I expand on specific trust-related concerns and identify ways to engender trust or, at the very least, make it easier to identify when we should in fact be less trusting of equipment or services which are available to Canadians and Canadian organizations.

Mitigating Supply Chain Dependencies

7. Supply chains can be turned against Canadians in several ways, but I will first address the risks linked with manufacturing or development dependencies. States, including China, have adopted industrial policies to protect and foster indigenous technology companies; Huawei, as one example, exists in part because of the Chinese government's policies to protect it.[3] The company produces equipment that is widely used around the world and sold at incredibly competitive rates, and the company enjoys reliable domestic revenue streams while also being able to offer low-cost loans from state-backed banks so that companies can acquire Huawei products at comparatively lower short- and long-term capital costs. The result is that Huawei, and other Chinese companies, have been able to prolifically expand into global markets with notable state support.
8. Contemporary and next-generation wireless telecommunications infrastructure will likely be mostly produced by Nokia and Ericsson, and Huawei, along with additional companies that will provide elements of 5G networking stacks. Networking equipment tends to be 'sticky', insofar as vendors often design their equipment to interoperate and the equipment tends to work less-efficiently with competitors' products. As a result, adopting one vendor's products at the outset of a major critical infrastructure outlay--such as 5G--can substantially lock-in the

[3] The company's founder stated, "[i]f there had been no government policy to protect [nationally owned companies], Huawei would no longer exist." See: Alberto F. De Toni. (2011). *International Operations Management, Lessons in Global Business*. London: Routledge, pp 128. Citing Xiao, 2002, p. 127.

vendor for subsequent elements of the network's upgrade path. Huawei equipment, in particular, has been noted as being very sticky; adopting the company's products now will increase costs to later integrate non-Huawei equipment into telecommunications networks.[4]

9. If Canadian companies are permitted to purchase Huawei equipment for their 5G networks, they may be fiscally motivated to do so. There is, however, a risk that the Chinese government might use dependencies on Huawei equipment to its advantages in future trade or diplomatic negotiations, or a vendor monoculture may result. In the former case, the Canadian government might be pressured to adopt 'China-friendly' policies so that Canadian companies could continue receiving equipment needed to stand-up or maintain their 5G networks or future 6G infrastructure. In the latter case, there is a risk that having just one vendor, or even just principally one vendor, supplying a given telecom network can increase the likelihood that a security vulnerability found in one device might then be replicated across all the vendor's same devices in a network. Scott Jones, Deputy Chief of Information Technology Security with the CSE, has raised this as a concern to the Standing Committee on Public Safety and National Security, when he stated that, "...you don't want one vendor and only one vendor. That makes you vulnerable across your entire spectrum and across all your telecommunications companies to the exact same vulnerability. You want to build in different vendors … That bakes in a large amount of security because you can't easily traverse up and down the so-called communications stack. That's one of the key elements for 5G".[5]
10. We would **recommend** that the government of Canada adopt a policy whereby no single vendor's products can compose an overwhelming majority of the equipment in a private telecommunications vendors' network. The intent of this is threefold. First, to reduce any foreign government's ability to leverage excessive dependencies on a vendor to accomplish diplomatic, trade, or defence negotiations. Second, this vendor-agnostic policy would impede the likelihood of vendor monocultures arising with the concurrent negative security properties. Third, doing so would encourage competition amongst telecommunications vendors and thus potentially reduce capital costs to Canadian telecommunications providers.
11. In the absence of indigenous technology companies, Canadians must depend on and trust products made by companies operating in Western Europe or Asia. To some extent, this is a normal result of globalization but, at the same time, it means that determining how to trust products now depends on assessments of foreign corporate suppliers based on foreign intelligence and considerations of foreign countries' national security laws, and how these laws might be applied to foreign companies' products, as well as based on conducting technical assessments of companies' products. In effect, there are a number of trust assessments that are made, inclusive of whether a product that is designed by a company in a Western nation and is at least partially manufactured in countries with opaque or less well understood national security laws, like China, should be considered more or less trustworthy products than those which are also almost entirely manufactured and shipped from China. Furthermore, even in the case of Western companies which produce telecommunications

[4] See: https://www.ncuscr.org/technology-regulation-industry-impact.
[5] See: https://hillnotes.ca/2020/02/13/5g-technology-opportunities-challenges-and-risks/

equipment[6] or provide social networking platforms history has shown that these companies can be co-opted by Western states' interests.[7]

12. Given the current state of manufacturing of products and delivering services, we **recommend** that any policies which are adopted to enhance trust in products and services remain vendor-agnostic, and be designed to recognize that obvious competitor nations and allied nations alike may be motivated to compel companies to adjust their products to achieve national aims.

Standards Setting and Internet Governance

13. At present, there are a small number of companies which are well positioned to provide 5G equipment. Unless significant changes occur this state of affairs is likely to persist when 6G infrastructures are ready to be deployed. Part of this is due to an industrial failure: Nortel is no more, and American companies in the infrastructure space have not focused on wireless standards and technologies to the same extent as their European and Chinese counterparts.
14. It may be largely too late for Canada to significantly influence the development of 5G standards, but the 6G working groups have already begun to meet. The Canadian government should actively encourage Canadian businesses and experts to participate in these working groups to, at the very least, ensure that security and privacy properties are aggressively baked into the standards as defaults.
15. We **recommend** that the Canadian government ensure that Canadian telecommunications providers enable all available security properties that are listed in the 5G standards, which are sometimes set to be voluntary to enable in the standards. This, in tandem with existing security policies, may enhance trust in the emerging 5G networks that Canadians will be using for decades to come.
16. We also **recommend** that the Canadian government explore ways of ensuring that Canadian interests are better represented during the 6G standards-setting processes, which are already underway. Specifically, the government could allocate tax incentives to corporations, as well as offer funding to non-governmental organizations or charities, so that Canadians and Canadian interests are more deeply embedded in standards development processes.
17. Furthermore, the government needs to carefully assess the efforts being undertaken at the International Telecommunications Union (ITU) and other standards bodies,[8] where efforts are being made by Huawei and the Chinese government to advance New IP, a protocol ostensibly intended to enable low-latency Internet of Things functionalities but which may also enable heightened surveillance and control of data within national borders.[9] To be blunt, these latter

[6] See as example: https://www.zdnet.com/article/congress-asks-juniper-for-the-results-of-its-2015-nsa-backdoor-investigation/.
[7] See as example: https://en.wikipedia.org/wiki/PRISM_(surveillance_program).
[8] Hoffmann, Stacie, Dominique Lazanski, and Emily Taylor. "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet." *Journal of Cyber Policy* 5, no. 2 (May 3, 2020): 239–64. https://doi.org/10.1080/23738871.2020.1805482.
[9] For more, see: https://oxil.uk/publications/2020-08-29-standardising-the-splinternet/.

properties may, if implemented, further enable authoritarian states to engage in domestic repression.

18. We **recommend** that the Canadian government continue to engage with its international partners and allies to carefully study New IP, to involve non-governmental experts in its ITU delegations which discuss New IP, and coordinate with allies in seeking to modify or oppose elements of the proposed standard which are likely to be abused to enhance authoritarian practices.

Incidental vs Deliberate Security Vulnerabilities

19. The complexity of contemporary digital systems means that software and hardware errors are accidentally, or incidentally, included into these systems. In some cases, these errors might be somewhat egregious (e.g., including old and known vulnerable code in a piece of software) or more akin to a spelling or grammar error (e.g., failing to properly delimit a block of code[10]). Regardless, individuals working for nation-states, private businesses, or in a personal capacity routinely look for these errors and may develop ways of using them to compel digital systems to behave contrary to their owners' or users' interests.
20. Separately, nation-states can compel organizations to inject vulnerabilities into hardware or software. In the past, equipment has been interdicted and modified before final delivery, encryption protocols weakened and propagated by standards bodies, and software deliberately modified to enable unauthorized activities. Just as Western governments have undertaken each of the aforementioned activities, there are fears that the Chinese government might use either its National Intelligence Law or Counter-Espionage Law to compel Chinese vendors to similarly modify products which are produced or manufactured in China before being delivered to foreign customers.
21. Allegations that Huawei has modified equipment before providing it to certain customers, while common, are not well founded in fact: to date there is little open source information that supports these claims, which have been made by the United States and other Western governments. While public analyses by the United Kingdom's Huawei Cyber Security Evaluation Centre (HCSEC) have revealed significant vulnerabilities in Huawei equipment, none are considered to have been deliberately inserted. The HCSEC's findings showcase the value of publicly auditing equipment that composes critical infrastructure. Notwithstanding the HCSEC's findings, the potential for hardware or software to be modified at state behest remains and the techniques which could be employed--such as modifying hardware components or introducing operating system instructions that state operators could take advantage of--remain plausible.
22. No single policy can alleviate risks posed by incidental or deliberate vulnerabilities. Some policies, however, can reduce the prevalence of incidental vulnerabilities and raise the cost of deliberately introducing vulnerabilities into digital systems.

[10] For more, see: https://www.wired.com/2014/02/gotofail/.

23. First, we **recommend** that organizations be required to provide a 'software bill of goods' for any critical infrastructure products, with the bill providing a structured identification of the software libraries and dependencies and their versions that are included in digital systems.[11] This would help organizations which audit digital code and dependencies to more quickly assess whether there were known pre-existing vulnerabilities in the codebase that underlies any given product. As an example, if an organization sold a telecommunications router and disclosed that they were using an outdated or vulnerable piece of software, it might be rejected for sale before entering the Canadian market. Should a vulnerability be found in an underlying software component after the device was sold then Canadian agencies could better determine which products sold in Canada were reliant on that component. This would not remediate all security issues but would provide information that is currently lacking in the Canadian or global marketplace.
24. In Canada, certain computer products are currently subject to the Common Criteria program,[12] where Canadian research labs and those of allied nations conduct formal security assessments of products, with more expensive (and relatively rarely performed) assessments evaluating whether products actually have the security properties they are formally asserted to possess. Canadian assessments of telecommunications equipment, inclusive of Huawei's, are draped in corporate and government secrecy, though they serve to discover and address at least some vulnerabilities.[13] The UK, in contrast, conducts more intensive assessments of Huawei equipment through its HCSEC and publicly releases its findings, which have repeatedly revealed critical incidental vulnerabilities that require remediation. There is no way for Canada to conduct assessments of all critical infrastructure on its own but the government could partner with allies to collectively assess critical infrastructure products and then publish their findings; in aggregate, their work would increase the likelihood of vulnerabilities being discovered and remediated, while also making it more challenging for state operators to deliberately have vulnerabilities designed into products purchased for use in Canada or by Canada's allies.
25. Second, we **recommend** that formal assessment frameworks and processes be created, preferably in tandem with friendly or allied nations, for classes of systems which compose Canadian critical infrastructure (e.g., telecommunications or energy systems) and that the Canadian government subsequently work to coordinate critical infrastructure assessments with its allies, and which are subsequently made public.
26. The Communications Security Establishment (CSE) presently uses an Equities Management Framework (EMF) to determine whether to retain vulnerabilities for its foreign intelligence, government assistance, and defensive or offensive cyber operations or, instead, disclose vulnerabilities to responsible vendors or communities to patch them.[14] At present, the framework leaves open the possibility that the Establishment may identify vulnerabilities either

[11] For more, see: https://www.ntia.gov/SBOM.
[12] For a listing of Common Criteria products, see: https://www.commoncriteriaportal.org/products/.
[13] For more, see: https://cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks.
[14] See: https://www.cse-cst.gc.ca/en/media/media-2019-03-08.

in the course of conducting assessments of equipment that is installed in Canadian networks or which is planned to be installed, or as a result of having Canadian researchers report vulnerabilities to the Canadian Centre for Cybersecurity in an effort to see vulnerabilities remediated. In cases where vulnerabilities are discovered in systems pertaining or related to critical infrastructure, or electronic devices which are significantly used by Canadians, the CSE should be required to disclose vulnerabilities to correct vulnerabilities and thus better ensure Canadians can better trust the devices and infrastructures they rely upon.

27. Third, we **recommend** that the Canadian government adopt a policy where it discloses all vulnerabilities in telecommunications equipment and other critical infrastructure, as well as vulnerabilities in significantly used personal devices, that are found in the course of information assurance activities that involve assessing equipment which may be installed into Canadian telecommunications networks, other critical infrastructure, or in electronic devices significantly used by Canadians and residents of Canada.
28. Fourth, we **recommend** that all vulnerabilities which are reported to the Canadian Centre for Cybersecurity be disclosed to responsible vendors or communities so that they may be patched, and never used by the CSE in furtherance of its foreign intelligence, government assistance, or defensive or offensive cyber operations prior to such disclosures taking place.

Chinese Social Media

29. Western countries have increasingly cast suspicious eyes towards Chinese social media platforms as they have expanded beyond Asia and become popular amongst western audiences. WeChat, as of 2019, had 1.15 billion users in China and internationally, with a reported 45 billion messages sent using the platform on a daily basis. Bytedance, the parent company of TikTok/Douyin, reported 1.29 billion active users in November 2020 with approximately 689 million of them using the TikTok service.[15] Whereas WeChat presently operates as a comprehensive digital platform in China, with miniprograms being used to massively extend the app's utility, many of its core features including WeChat Pay are increasingly being used in Canada. TikTok, in contrast, continues to principally offer its core functionality: letting individuals create and view short content, while algorithmically assessing content they may prefer based on past views and decisions made by TikTok staff.
30. As with other hardware and software companies located in China, social media platform companies must adhere to state national security and counter-espionage legislation. Past Citizen Lab research has showcased there is considerable variation between how companies implement censorship on their platforms and, also, that platforms have often evolved how they monitor, censor, and take down information which is disclosed on their platforms.
31. Legislators and government agencies throughout the West are increasingly raising concerns about both of these platforms. In the case of WeChat, Citizen Lab research has revealed that even international users of the platform who register their accounts outside of China and use non-Chinese phone numbers can have their content subject to political surveillance that,

[15] See: https://backlinko.com/tiktok-users.

subsequently, is used to develop political censorship for Chinese WeChat users.[16] The same research project found that WeChat's public terms of service and privacy policies did not disclose these activities were taking place, and that efforts to utilize Canadian privacy laws to better understand the nature of this surveillance were fruitless. Toronto Star journalist Joanna Chiu has noted in her reporting that Canadian content, such as about Meng Wanzhou, has been blocked in the past while memes supporting the detainment of Michael Kovrig have been permitted to be posted and shared.[17] CSIS has warned MPs to avoid using WeChat for nebulous cybersecurity risks.[18] Separately, during the last federal election Tencent did not produce a digital advertising registry as required under Canadian law, while still accepting political advertisements.[19] Furthermore, a publication by the Australian Strategic Policy Institute (ASPI) collected examples where WeChat users outside of China, such as public posts of foreign embassies, remain subject to censorship. The same report also showcased examples where Chinese authorities have threatened individuals to self-censor or else risk their families suffering ill consequences.[20]

32. In the case of TikTok, there have been at least two principal sets of concerns.[21] First, there is a worry about large volumes of user information being collected by the application and subsequently being used in the near-present or future to facilitate Chinese information security or foreign intelligence operations. These worries are premised on the idea that data TikTok collects, which are reminiscent of Western social media companies' collections, could be useful in state digital targeting operations. Second, there is a worry that TikTok's content presentation algorithms could be used as part of influence operations to develop positive perceptions of China by promoting some content and preventing Western users from accessing other content. The aforementioned report by ASPI summarizes cases where this has occurred to date, inclusive of some LBGTQ+ content being shadowbanned (i.e., content can be posted to the service but is largely or entirely hidden from other users), some material pertaining to protests in the United States around defunding police forces, and promoting pro-China content about Xinjiang. In August 2020 the Chinese government added content-recommendation algorithms to its export control list in response to American efforts to force TikTok to sell or disclose its content promotion algorithms (amongst other efforts).
33. While the Trump administration sought to impede the operation of WeChat and TikTok in the United States the efforts have, to date, been ineffective. In Canada there have not been any equivalent efforts to prevent Canadians or residents of Canada from using the applications. At present, blocking these companies from providing services likely represents a gross

[16] See: https://citizenlab.ca/2020/05/we-chat-they-watch/.
[17] See: https://www.vice.com/en/article/zmana5/experts-say-we-should-watch-out-for-wechats-influence-in-canadas-election.
[18] See: https://ipolitics.ca/2019/07/05/mps-staff-warned-not-to-use-chinese-app-wechat-due-to-cybersecurity-risks/.
[19] See: https://www.cbc.ca/news/politics/wechat-election-social-media-1.5318589.
[20] See: https://www.aspi.org.au/report/tiktok-wechat.
[21] For an American-focused, and more detailed, discussion see: https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks.

overreach when balanced against any actual risks posed by the services. However, the Canadian government could require all social media platforms, including Chinese platforms, to comply with a set of requirements in order to continue lawfully operating in Canada and to better understand how these companies operate with regards to user data and compliance with government requests for data or modification of platforms' delivery of content.

34. First, we **recommend** that companies be required to publish their content moderation guidelines, which should explain where content moderators are located, how moderation guidelines comport with domestic law, and processes that are undertaken during moderation activities. As part of these guidelines, companies should be required to explain how they use algorithmic and human processes to identify and restrict access to, or take down, content.
35. Second, we **recommend** that companies be required to publish guidelines that explain the ways in which their platforms are subject to state-mandated surveillance and, if relevant, censorship. This should include a detailed description of relevant laws as they are operationalized by the platform, any and all processes that the organization has in place to dispute efforts to surveil or censor content, explanations of how individuals are notified that their content has been placed into the platform's surveillance or censorship processes, and detailed explanations with examples of how certain content violate which specific articles of content laws or regulations.
36. Third, we **recommend** that organizations be required to publish their government agency security and access guidelines, which explain how and under what circumstances an organization will respond to orders or requests from state agencies. Such guidelines should explain how the organization responds to requests from the government where its headquarters is located, as well as requests issued by international authorities such as those in Canada. It should make clear the processes which are in place to protect the platform's users and communities.
37. Fourth, we **recommend** that organizations be required to publish transparency reports. Such reports should indicate the regularity at which government authorities make requests for user information, the grounds for the requests, the responsiveness of the organization to the requests, and the amounts and kinds of data which are disclosed. Such reports should also include information about the number of times that authorities have either directly requested specific content to be taken down or shadowbanned, as well as whether government agencies have required specific classes or types of information to be blocked, taken down, or shadowbanned. This latter class of information might include political information, information pertaining to LGBTQ+ rights, foreign affairs, or other typologies to be developed in association with international civil liberties organizations.
38. Fifth, we **recommend** that organizations be required to make their algorithms available for government audit in situations where there is reason to suspect that they are being used to block, censor, or shadowban lawful communications in Canada, or they are being used to facilitate influence operations in Canada, or they are otherwise being used to interfere in Canada's domestic operations or international relations.
39. Sixth, we **recommend** that organizations be required to disclose whether, under what conditions, and how they share information about users or content on their platform among their headquarters and regional offices, in particular where either the organization's

headquarters or regional offices operate in jurisdictions with poor human rights records, due process records, or privacy protection laws or practices.

Concluding Remarks

40. The aforementioned recommendations are meant to better ensure that Canadians can trust the critical infrastructure, electronic devices, and digital services and platforms that they rely upon in their daily lives. While these comments are submitted in the context of risks posed by the Chinese government, it is noteworthy to recognize that the most significant cybersecurity and intelligence threat that has been discovered in the past several months is the result of Russian and Chinese operators alike penetrating the SolarWinds Network Performance Monitor and, subsequently, moving into sensitive organizations' networks which utilized SolarWinds' products. That SolarWinds was an American-operated organization did not inherently make their product any more secure or resilient from foreign intelligence operations than those developed or manufactured in an authoritarian country.
41. In effect, any positions which are adopted by the Canadian government must recognize that threat actors search for vulnerabilities that exist in products, with little care for where those products are developed or produced. Consequently, we would encourage this committee to carefully assess any recommendations that it ultimately decides upon with the aim of ensuring that they will not just affect Chinese companies or companies with operations in China and, instead, work to enhance the security built into all critical infrastructure technologies, electronic devices used by Canadians and residents of Canada, and digital services which they rely upon. Only by broadly improving the security integrated into contemporary technologies will everyone in Canada be made safer than they are now from foreign and domestic operators who are working contrary to Canada's domestic and foreign interests.

Organizational Information

42. The views I have presented are my own and based out of research that I and my colleagues have carried out at my place of employment, the Citizen Lab. The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.
43. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.