Appearance before the Special Committee on Canada-China Relations, March 22, 2021

Good evening. My name is Christopher Parsons. I am a Senior Research Associate at the Citizen Lab, which is part of the Munk School of Global Affairs & Public Policy at the University of Toronto. I appear before this committee in a professional capacity that represents my views and those of the Citizen Lab, and comments are based on our research into Chinese technology companies.

In my time I want to point to some ways by which we can develop trust in the products and services that are manufactured in, transited through, or operated from China. I do so by first turning to the issue of supply chain dependencies.

Mitigating Supply Chain Dependencies

A rising concern is the extent to which Canadian companies, such as our telecoms, might become dependent on products made by Chinese companies, such as Huawei. Dependency runs the risk of generating monocultures, or cases in which a single company dominantes a Canadian organization's infrastructure. In such cases, up to three risks can arise.

First, monocultures can enable foreign governments to leverage dependencies on a vendor to apply pressure in diplomatic, trade, or defence negotiations.

Second, monocultures can create a path dependency, and especially in 5G telecommunications environments where there is often a degree of vendor lock-in built into vendors' telecom equipment.

Third, monocultures risk hindering competition amongst telecommunications vendors, to the effect of increasing capital costs to Canadian telecommunications providers.

All of these challenges can, in part, be mediated by requiring diversity in Canadian telecommunications companies' networks, as has been recommended in the past by the CSE's Deputy Chief of Information Technology Security, Scott Jones. In this case, trust would come from not placing absolute trust in any given infrastructure vendor.

I now turn to building trust in software and hardware systems more generally.

Addressing Incidental and Deliberate Technical Vulnerabilities

Software and hardware errors are often incidentally placed in digital systems. Some are egregious, such as including old and known vulnerable code in a piece of software, and others more akin to spelling or grammar errors, such as failing to properly delimit a block of code. There are also limited situations where state agencies compel private companies to inject vulnerabilities into their products or services to enable espionage or attack operations.

No single policy can alleviate all the risks posed by vulnerabilities. However, some can enhance trust by reducing the prevalence of incidental vulnerabilities and raising the cost of deliberately injecting vulnerabilities into digital systems.

Some trust enhancing policies include:

First, companies could be required to provide a ‘bill of goods’ that declares products’ software libraries and dependencies, and their versions. This would help to ensure that known-deficient code isn’t in critical infrastructure and also help responders identify vulnerable systems upon any later discovery of vulnerabilities in the libraries or dependencies.

Second, Canada and its allies could improve on existing critical infrastructure assessments by building assessment centres that complement the UK’s, which presently assesses Huawei equipment. Working collectively with our allies we would be better able to find incidental vulnerabilities while raising the likelihood of discovering state adversaries’ attempts to deliberately slip vulnerabilities into systems’ codebases.

Third, Canada could adopt robust policies and processes to ensure that government agencies disclose vulnerabilities in critical infrastructure to appropriate vendors and communities, as opposed to potentially secretly hoarding them for signals intelligence or cyber operations.

I now briefly turn to increasing trust in Chinese social media platforms.

Regulating Social Media Platforms

Citizen Lab research has shown that WeChat has previously placed Canadians’ communications under political surveillance to subsequently develop censor lists that are applied to China-registered WeChat accounts. Our research on TikTok, released today, revealed that there is no apparent political censorship or untoward surveillance of Canadians communications on that platform.

Based on our findings, we suggest that social media companies be required to publish more information on their activities to enhance trust.

This would include publishing detailed content moderation guides, publishing how and why companies engage in monitoring and censoring behaviours, publishing how organizations interact with government agencies and address their corresponding demands, and publishing annual transparency reports that detail the regularity and effects of state and non-state actors who make requests for users’ data.

Platforms could also be compelled to make available algorithms for government audit where there is reason to suspect that they are being used to block or suppress lawful communications in Canada, or they are being used to facilitate influence operations. Platforms could also be compelled to disclose when user data flows through, or is accessible by, parts of their organizations which have problematic human rights, data protection, or rule of law histories.

Conclusion

To conclude, we believe that the aforementioned sets of recommendations would ameliorate some of the cyber-related risks linked with Chinese supply chain management and social media platforms. More broadly, we believe that these policies should be applied in vendor- and country-agnostic ways to broadly improve trust in digital systems. Further, the brief that we submitted to this committee provides additional details and recommendations, especially as applied to governing Internet standards.

Thank you for your time, and I look forward to your questions.