Are Canadians prepared for cyberattacks in the Second Cold War?

We have seen reliable evidence and reports showing that the Chinese Communist Party (CCP) is committing crimes against humanity targeting members of the Uyghur minority group. The CCP is also waging a crackdown on human rights in Hong Kong by arresting journalists, scholars, pro-democracy legislators and advocates for freedom. Beyond its borders China has adopted policies that are provocative and meant to intimidate neighboring countries across the South China Sea and near Taiwan. The Five-Eyes (U.S., U.K., Canada, Australia and New Zealand) cannot acquiesce but must take a hardline stance against the spread of China's totalitarian influence.

As tensions grow, a Second Cold War is on the horizon. Unlike the First Cold War against the Soviet Bloc, this emerging conflict opens a new field of combat in cyberspace. The resources essential to modern living: power generation, communications, transportation, food supplies, could become vulnerable to cyberattacks. Canadians need to be aware that the threat of catastrophic upheaval of their lives is real and significant. The question is: Are Canada's critical infrastructures sufficiently fortified to deflect a massive cyberattack?

Risks in critical cyber-physical systems. Most people associate the threat of cyberattacks with their electronic devices and online accounts. In fact, the disabling of critical infrastructures under cyberattacks would go much further. The systems used for power generation, water supply, public transportation, healthcare facilities, banking and trading would be paralyzed. It's taken the world just two decades to reach the point where the most vital systems needed for the smooth functioning of the modern world, have become connected to the cyberworld, facilitating real-time remote access, monitoring and control.

New generations of control systems may improve operational efficiency, but as targets for hostile agencies intent on bringing the modern world to a standstill, these cyber-physical systems are ideal. The chaos alone would cost many lives and properties. Cyberattacks are but one part of the strategy for massive "unrestricted warfare," proposed by China's People's Liberation Army.

Risks of silent information collection. The precursors to a large-scale cyberattack may take place out of view. They may have already crept in without our notice. Canadian Internet Service Providers (ISPs) are inaugurating their 5G networks, introducing innovative artificial intelligence (AI)-powered applications and devices attached to the Internet-of-Things (IoTs). With the evolution of new systems will come the gathering of even more personal online and offline data which will be integrated for "more customized" services in our smart cities. These infrastructures, if ever compromised, will become even more deeply engaged in data collection of citizens. Already, it is reported that the CCP actively collects data of foreigners. The *Zhenhua Data Leak of 2020* revealed that a Chinese state-owned military company monitoring more than 2.4 million people, globally, including Americans, Canadians, Britons and Australians. That information is capable of innumerable applications, including blackmail of people in sensitive positions, especially politicians, scientists and executives of major business interests.

How well are we prepared for cyberattacks? Obviously not well. In 2020 the Communications Security Establishment (CSE) warned that state-sponsored organizations "are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals." *The National Post* reported that Canada allocated $144.9 million in 2019 to protect Canada's critical cyber infrastructures. To date, however, there has been no concrete actions to safeguard Canada's systems.

Civil organizations, corporations and individuals are not well prepared, either. Take a look at the hardware and software components at your workplace or school. You are likely to find component parts manufactured by foreign state-owned or related companies. Some state-owned companies may furnish an interface of American or Canadian company, but the core development team and data centers remain in China. This implies that on demand the hardware and software producers are obliged to surrender their data to the Chinese government under the mandate of China's Cybersecurity Law.

Critical cyber-physical systems are complex. They consist of layers interconnected hardware and software components created by different vendors. People may ask why we don't just validate their security before using them. Security verification may be important, but it is insufficient. Many critical cyber-physical systems require continuous updates, as fresh vulnerabilities are exposed. Software vendors easily can inject fresh lines of code to create a backdoor allowing access to the system. During the new Cold War era, it is vital that our critical infrastructures are not vulnerable to attack from systems continuously updated by foreign state-owned companies.

What can we do? Canadian agencies, corporations and civil organizations should review their critical infrastructures and re-evaluate risk potential. I believe Canadian companies and organizations have the will to safeguard their infrastructures and data, but lack the resources and expertise to identify state-sponsored companies. It would be of great help if the Canadian government were to publish a list of state-sponsored companies. At the individual level, you are wise to stay away from social network and communications apps developed by foreign state-controlled companies.

Benjamin Fung is a professor and Canada Research Chair in Data Mining for Cybersecurity at McGill University.

(This is the preprint version. The official version was published in *The Hill Times* on 2021/05/05.)