UNIVERSITY OF CALGARY | THE SCHOOL OF PUBLIC POLICY

Canada and cyberwarfare. Are we ready to attack?
New School of Public Policy report

For Immediate Release June 12th, 2019

Calgary – The Canadian government is now openly discussing the possibility of making cyberweapons part of its official national defence strategy as revealed in a recent government white paper, entitled "Strong, Secure, and Engaged" (SSE). This direction not only opens up new possibilities for Canadian defence, it could also represent significant new risks. Without good answers to the difficult questions this new direction could raise, the country could be headed down a very precarious path.

Today, The School of Public Policy with CGAI and author Ken Barker released a report that examines the world of cyberwarfare, the new possibilities for Canadian defence and next steps to ensure our security while avoiding the most serious consequences.

According to Barker "Cyberweapons do offer unique benefits. Since they tend to be far less costly to deploy than kinetic weapons — such as missiles, bombs and guns — they can level the playing field between richer, stronger states and weaker, poorer ones. Larger states may even be at further disadvantage by relying on larger, more sophisticated computer systems that could become a liability if successfully attacked. Cyberweapons also possess risks of unintended consequences and have a much greater potential to impact targets that were not intended by the attacker."

Launching a cyberweapon to disable an enemy's supply-chain computer systems and accidentally infecting its nuclear systems, setting off a nuclear incident, is a terrifying scenario. It might even rise to the level of a war crime. There are no international treaties governing the use of cyberweapons. If Canada engages in cyberwarfare without one, there will be no formal limits on what actions are acceptable and what actions are not.

There are many discussions that still must be had within Canada and beyond to mitigate the risk of pursuing cyberweapons. Potential next steps should include: Defining the goals of a cyberattack strategy; the rules of engagement must be clearly defined; who is authorized to use cyberweapons either in peace or wartime? Rules of war need to be defined for cyberweapons and finally, having a partnership with cybersecurity stakeholders.

It is unclear even whether a prime minister or Parliament will be qualified to safely declare cyberwarfare, given its technical complexity. These are just some of the debates we need to have before Canada decides to embark on developing cyberwarfare capabilities. Now is a good time for those debates to start.

The paper can be downloaded at https://www.policyschool.ca/publications/

-30-

Media contact:
Morten Paulsen
morten.paulsen2@ucalgary.ca
403.220.2540