THE HILL TIMES
THIRTY-FIRST YEAR — CANADA'S POLITICS AND GOVERNMENT NEWSPAPER — WEDNESDAY, MARCH 4, 2020 $5.00

Global

How Canada can succeed in the cyber century

Washington and Westminster concluded that effective cyberdefence requires not only new approaches but a different worldview when interacting with the private sector, says Christyn Cianfarani of CADSI.

In cyber, governments are just beginning to come to grips with what the industry looks like, let alone the technologies those firms produce. *The Hill Times photograph by Andrew Meade*

BY CHRISTYN CIANFARANI

One of Ottawa's worst-kept secrets occurred a few years ago when the National Research Council's networks were hacked by a foreign adversary, resulting in the sweeping theft of its intellectual property and an estimated financial cost in the hundreds of millions of dollars. A couple of years earlier, the Department of Finance and Treasury Board Secretariat suffered a foreign cyberattack that compromised systems to such a degree that internet access in those departments was shut off for weeks.

We know something about these attacks largely by accident—governments and truth be told, businesses, don't like to acknowledge when their systems have been compromised, and for good reason. But they are not isolated incidents. Rather, they are the face of cyber warfare and espionage in the 21st century.

Most countries have access to advanced cyberweapons because they are relatively cheap to develop and deploy. Unlike conventional or nuclear arms, you don't need billions of dollars, an army of engineers, or huge, integrated corporations to produce cyberweapons. A small firm with a few crack employees—or a troll factory—can invent and launch a cyber weapon as devastating in its impacts as anything the world's largest industrial firms can produce.

Companies dominate the cyberdomain in a way they do not in traditional defence technologies, and this is the central challenge governments face.

The private sector, not the government, owns most of the world's digital infrastructure, the conduit for cyberattack. There is no other domain in which the private sector—often very small companies that few people have ever heard of, located in places you wouldn't expect—is capable of producing technologies that can cripple (or protect) not just militaries in the field, but entire economies and societies. Former FBI director James Comey summed up the basic sentiment when he said, "The private sector is the key player in cybersecurity … they possess the information, the expertise and the knowledge to address cyber intrusions and cybercrime in general."

With conventional or nuclear weapons, governments know all the companies that produce the technologies, and they utilize, influence, and sometimes control those firms in the national interest. In cyber, governments are just beginning to come to grips with what the industry looks like, let alone the technologies those firms produce. And the challenge is immense because those companies and technologies are rapidly changing.

Innovation has become a buzzword of our times. In cyber, however, it defines the space. Product lifecycles are measured in weeks, not years or decades, as they are in conventional defence technology. Technological obsolescence occurs daily. Economist Joseph Schumpeter's concept of "creative destruction" accurately describes the cyber domain, where the entrepreneur is the innovator and disruptive force changing the game for small and large firms alike. It is a pace of change that democratic governments and militaries are incapable of keeping up with on their own.

Canada's allies, notably the British and the Americans, recognized years ago the unique nature and paradigm-shifting impact of cyber technology on national security. Consequently, both Washington and Westminster concluded that effective cyberdefence requires not only new approaches but a different worldview when interacting with the private sector, where the majority of innovation happens, and where deep pools of expertise in offensive and defensive cyber technologies reside.

The American and British governments have found ways to integrate industry with government efforts to combat cyberthreats. In those jurisdictions, we often see joint government/industry teams, with equal representation from public and private sectors, working collaboratively—through strategic dialogue at one end to talent exchanges of key personnel at the other. Specific programs have been developed to reach into industry to extract knowledge, expertise and technology in the service of national security.

None of this is happening in Canada today.

If there is one word that sums up what it will take to successfully defend against cyberwarfare, cybercrime and succeed in the cyber century, it is collaboration. Our allies and adversaries know this and have found creative ways for government and industry to collaborate in this dynamic and innovation-intensive domain. It is high time the Canadian government does likewise.

Christyn Cianfarani is the president and CEO of Canadian Association of Defence and Security Industries.

The Hill Times