Welcome to CSIS

In today’s world, it may be that the first line of defence in protecting national security is public awareness of the threat environment. Security is a collaborative effort between governments and citizens, and in that spirit we at CSIS see the value in transparency, to the extent such is possible. It is an axiom within intelligence services that successes are known only to us but failures are known to all. In between those two poles, there is much that can be shared.

For example, in recent years there has been an exponential increase in public awareness of the cyber threat, a realization that if you open even one malicious e-mail hostile actors can steal your most sensitive information – and do so in a blink of an eye and from thousands of kilometers away. CSIS and its partners are mandated to protect Canada’s security interests. Our job becomes immeasurably easier as ordinary Canadians learn to be more careful where they click.

The sophistication and determination of cyber-spies, some of whom are backed by foreign governments, will continue to grow. Individuals, corporations and nations that are unable to defend themselves will suffer economic and other consequences. Fortunately Canada is well-positioned to meet this very serious threat.

Despite the visibility attached to cybersecurity, terrorism is still our greatest preoccupation. The goal of terrorists is not to steal secrets in the countries they target but to kill people. This remains an immediate danger to public safety.

Terrorism is a multifaceted phenomenon, one that has evolved since the CSIS Act was conceived nearly 30 years ago. In the heyday of political terrorism, a terrorist’s objective was more often than not to draw attention or support for a cause, rather than to maximize civilian casualties. Those were the days when violent groups issued demands and even gave advance warning. In executing the 9-11 attacks, by contrast, the hijackers made no demands and Al-Qaeda initially did not even claim responsibility. Similarly, the contemporary phenomenon of “lone actor” terrorism – manifested most horrifically in 2011 by Anders Breivik in Norway – seems to have as its objective the murder of as many people as possible.

Moreover, modern technologies have accelerated the speed with which threats develop. The time between the conception and execution of an attack can be very short. When it comes to counter-terrorism, CSIS operates in a higher risk environment than ever before, with no margin for error. The sad reality of Canadian citizens participating in terrorist activities is another aspect of the problem that is rightly drawing public attention.

That said, one of the most disturbing national security incidents in recent times was not terrorism. In January 2012, Sub-Lieutenant Jeffrey Paul Delisle was arrested in Halifax and charged with spying for a foreign government. He later pleaded guilty and received 20 years in prison.

The case was historic because it marked the first conviction under the Security of Information Act and served as a reminder that Canada is a highly attractive target for hostile intelligence agencies. There are as many, and arguably more, attempts to steal Canadian secrets today – economic, military, political – than at any time in our national history.

As with counter-terrorism, our counter-espionage units operate in a higher risk environment than ever before. In the age of thumb drives, a warehouse of documents can be stolen in the blink of an eye and then carried away in one’s pocket. As CSIS has said before, we wish for a world where the methods by which Canadian interests are harmed were diminishing rather than expanding, but sadly that is not the world we know.

The professionalism of CSIS is reflected in the fusion of operational effectiveness and responsible administration. We appreciate the confidence the government invests in the Service, and it remains for us a privilege to protect Canadians and Canada’s interests.

Michel Coulombe