CYBER SECURITY

ISSUE

Canada's international approach to cyber security.

CANADIAN POSITION

- The greatest cyber threat to Canadian national interests comes from state and state-sponsored actors targeting Canadian government systems, critical infrastructure and intellectual property.
- Addressing these threats requires better security at home, but also coordinated action with friends and partners to reduce the threat that emanates from abroad and to build resilience. To this end, Canada supports the development and implementation of likeminded initiatives to hold hostile states to account and impose costs on them, in accordance with international law.

BACKGROUND

Cyber Security

Cyber security is one of the most serious economic and national security challenges that Canada faces. The fast-evolving cyber threat environment now includes new risks and challenges from both state and non-state actors, such as hostile governments and their proxies. Certain states actively pursue their interests in cyberspace through espionage, the theft of intellectual property and sensitive information, among other means. Some states are pursuing military cyber capabilities, as well as seeking to censor, control and partition the Internet under the pretext of cyber security. Defending Canada against cyber threats is a shared responsibility; it cannot be achieved by the Canadian government alone. For this reason, Canada is continuously working with friends and partners to enhance cyber security by identifying cyber threats and vulnerabilities, and by preparing to respond to a broad range of cyber incidents based on a shared understanding of international law.

Domestically, Canada has committed to playing a strong leadership role in order to strengthen Canada's cyber security and to protect and advance Canada's national security and economic interests. In October 2010, Public Safety Canada released Canada's Cyber Security Strategy and Action Plan to secure Government of Canada cyber systems, enhance partnerships to secure vital cyber systems outside the federal government, protect Canadians as they connect online, as well as enhance the detection of, and ability to response to, continually evolving cyber threats. Public Safety has led the effort to update the Strategy, s.69(1)(g)re(c) and is expected to be published shortly. Cyber issues were also addressed as part of the recent Defence Policy Review. Canada's new defence policy that was released on June 7, 2017 stated that the Canadian Forces will develop the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions.

Internationally, Canada collaborates with close friends and partners that share the same vision for a free, open and secure Internet in order to promote cyberspace as a platform for political, social and economic development, which opposes efforts of repressive regimes to control the Internet and its content. Canada believes that international law is applicable and is essential in maintaining peace and stability in cyberspace. In addition, Canada has been advocating for voluntary norms for state behaviour in cyberspace in bilateral and multilateral engagement. The

applicability of international law in cyberspace and complementary cyber norms were recognized in the 2013 and 2015 reports of the UN Group of Government Experts (UN GGE) on international cyber issues, in which Canada participated along with the US. Last year as a result of Russian, Chinese and G77 intransigence, the UN GGE process failed to develop a consensus report that recognized the applicability of international law and the importance of voluntary norms of state behaviour in cyberspace. Due to a growing sense of urgency, likeminded states are shifting emphasis to establishing a likeminded deterrence and response strategy to address malicious cyber acts. Canada is actively engaged in these efforts and continues to advocate for greater awareness and implementation of international law, voluntary cyber norms, and confidence building measures to enhance stability in cyberspace, in close coordination with key allies including the US.

Cyber Attacks

Malicious state-sponsored acts affecting national security interests are increasing, although none, to date, have met the threshold of the "use of force" under international law. For example, Russia hacked the US Democratic National Committee over the summer of 2016 and the US Office of Personnel Management was hacked in 2015 by China. Also in 2015, the Canadian government publicly attributed the hacking of the National Research Council to China.

Systems outside the Canadian government, but of national interest, are also subject to such malicious cyber activities. For example, the World Anti-Doping Agency (WADA), based in Montreal, was recently hacked by a suspected state-sponsored actor, apparently for political reasons. Private information about several athletes was subsequently leaked.

Likeminded countries have been increasingly working together to respond to recent malicious activities by foreign actors, including hostile states and their proxies. Last December, Canada supported the US call to join Five Eyes partners to publicly assign responsibility to North Korean actors for the WannaCry ransomware attack that paralyzed UK hospitals. In February this year, Canada joined likeminded countries in assigning responsibility to Russian actors for the NotPetya cyber outbreaks of July 2017 that caused massive damage to government and business networks, primarily in Ukraine, but also more widely.

KEY MESSAGES

- Canada is committed to promoting international stability in cyberspace, as well as to promoting a free, open and secure cyberspace.
- The threat posed by malicious acts in cyberspace is real and growing.
- The Government of Canada believes that peace and stability in cyber space is grounded on the acceptance of the applicability of existing international law – that requires states to resolve disputes peacefully, but also provides a legal basis for self-defence and counter-measures. It also depends on the cooperative development of voluntary norms of state behaviour and the implementation of confidence building measures.
- Together with friends and partners, Canada is committed to deterring malicious cyber acts, and responding when they occur. This includes clear statements to identify those responsible based firmly in international law and agreed [established] norms of state behaviour – and agreed strategies drawing on a range of diplomatic and other tools to respond proportionately to malicious acts by those who would do us harm.