Calls for Canada to develop cyberwar capabilities

Dylan Lubao
13 September 2016

Canada's spy agencies and military should be upgraded to better carry out offensive cyber warfare attacks against "foreign adversaries," a strategy paper published in July by a Canadian military think tank argued.

Titled "Canada and Cyber Warfare," and written by retired Major General John Adams for the Canadian Global Affairs Institute (CGAI), the paper urges that Canada improve its capability to infiltrate, disrupt and destroy the computer networks of its foreign rivals.

Adams is the former head of the Communications Security Establishment (CSE), the country's signals intelligence service. He has been a leading spokesman for the drive to expand the domestic and foreign powers of both CSE and the Canadian Security Intelligence Service (CSIS), Canada's domestic spy agency. Adams has previously boasted of CSE's deep integration in the US National Security Agency's illegal spy operations, with the aim of "mastering the internet."

The basic arguments Adams puts forward in his paper have been used time and again to push for greater powers for the spy agencies and sweeping attacks on democratic rights. Vague and unsubstantiated claims are made about cyberattacks on sensitive computer infrastructure by foreign governments or terrorist groups—attacks which are supposedly difficult for Canada to fend off due to outdated equipment or legal barriers.

Other high-ranking former members of Canada's national security apparatus have also weighed in. Ray Boisvert, a former Assistant Director of CSIS, has complained that Canada's cyber warfare capabilities remain "rudimentary at best" and woefully underfunded.

The mounting demands for Canada to develop offensive cyber warfare capabilities are rooted in the growing tensions between the major powers internationally and the realization within Canada's ruling elite that to assert its imperialist interests it must prepare for war.

In recent years, the United States has frequently resorted to claims of cyberattacks from hostile countries to stoke tensions with its geopolitical rivals, above all Russia and China. President Obama unveiled a vast array of new cyber policing powers last year to tackle alleged threats, while earlier this year Germany established a new department in its Defence Ministry and created a new branch of its military to wage cyberwar, including offensive operations. (See: German army prepares for cyberwar)

Adams' paper defines cyberspace as a domain comprised of the internet and other network infrastructure used by governments, militaries, corporations, and other organizations to maintain the ever-expanding scope of "modern civilization." It notes that cyberspace has "become the centre of gravity for the globalized world ... including military operations."

It goes on to state that cyberspace has "become an emerging theatre of operations," with successful attacks capable of crippling "the ability of states to function." Adams presents cyber warfare as inherently "cheaper, cleaner and less risky for an attacker" and so capable of crippling target infrastructure that it may soon supersede physical warfare.

Cyber warfare is typically defined as falling into one of three categories:

• Computer network attacks: designed to disrupt, deny, degrade or destroy computer networks or the computers themselves

• Computer network exploitation: seizing intelligence-grade data

• Computer network defence: measures taken to protect one's networks from cyberattacks

Adams, Boisvert and others are emphasizing the need to provide the spy agencies and the Canadian Armed Forces (CAF) with the resources and the mandate "to direct offensive action, in the form of cyber attacks," something Adams laments they have lacked up to now. Failure to do

so, warns Adams, would be “neglectful beyond belief.”

Adams’ CGAI paper is directed at influencing the government’s Defence Policy Review, which in its “public consultation” paper itself raises the issue of how Canada should respond to the growing importance of cyber warfare.

Launched at the beginning of April, the review is the first in more than two decades. It is being used by the Trudeau Liberal government, the military-security establishment, and the corporate and financial elite to push for major hikes in military spending, the procurement of a vast array of new warplanes, battleships, submarines, and high tech weapons, and more aggressive use of the military to secure Canadian imperialism’s predatory interests.

In their ten months in office, the Liberals have dramatically expanded Canada’s participation in all three of Washington’s major geostrategic offensives—in the Middle East, where the US is seeking to overthrow Syria’s government as part of its drive to secure unchallenged domination of the world’s most important oil producing region; against Russia; and against China.

In July, Trudeau announced that Canada would take the leadership and provide the bulk of the troops for one of four new NATO battalions being deployed on Russia’s borders in Eastern Europe. Under Trudeau’s government, Canada has also repeatedly voiced its support for the US’ provocative stance on the South China Sea dispute and expanded military-security ties with Washington’s closest ally in the Asia-Pacific, Japan

By posing the question of the type and size of investments required for cyber warfare systems, and the need to maintain interoperability with “key allies,” the Defence Policy Review consultation paper makes clear that the Liberals are also dead set on rapidly arming the spy agencies and military for offensive cyber warfare operations.

An example of the type of cyber warfare operations being considered is provided by the example of the 2010 Stuxnet virus, which was developed and deployed by a joint US-Israeli espionage team to target the computer-controlled gas centrifuges at Iran’s Natanz uranium enrichment plant. The virus reportedly caused hundreds of the centrifuges to self-destruct.

As one of the closest military allies of the US, Canadian cyber warfare units would undeniably be on the front lines in a war between Washington and its current main rivals, Russia and China.

While levelling accusations of cyber espionage against its rivals, the Pentagon established its own Cyber Command in 2010 for the express purpose of carrying out cyberwar against them.

As for the claims that Canada’s cyberwar capabilities are defence-oriented and inadequate, nothing could be further from the truth.

CSE has been integrated with the NSA for decades, playing a critical role in eavesdropping on the Soviet Union during the Cold War. During the invasion and occupation of Afghanistan, CSE boasted of its role in providing crucial military intelligence to the CAF.

More recently, CSE was exposed by NSA whistleblower Edward Snowden as a main auxiliary of the NSA in spying on foreign governments. Through the agency’s LANDMARK software, CSE can hack thousands of foreign computers in a matter of hours and remain essentially untraceable.

In 2013, it was revealed that CSE established covert off-shore sites at the request of the NSA to conduct surveillance on at least 20 “high-priority” countries. Among the foreign governments surveilled were Brazil, over its disputes with Canadian corporations, and Kenya, in which a cellphone network was infiltrated at the request of the British Government Communications Headquarters (GCHQ) spy agency.

Former NSA executive Thomas Drake summed up one of the reasons CSE is a valued NSA partner: “Think of certain foreign agreements or relationships that Canada actually enjoys that the United States doesn’t, and under the cover of those relationships, guess what you can conduct?”

Also being planned is deeper integration of CSE, CSIS, the Royal Canadian Mounted Police (RCMP), and the CAF. Under a five-year plan initiated in 2013, these four entities are to be brought under the umbrella of the Canadian Joint Operations Command (CJOC), the CAF’s central command and control hub. CJOC directs both domestic and foreign missions, and is involved in cyber support for all three branches of the military.