Canada to wage offensive cyberwar

Laurent Lafrance
12 July 2017

Justin Trudeau's Liberal government has ordered the Canadian military and the country's signals intelligence agency, the Communications Security Establishment or CSE, to collaborate in the development of cyberwar capabilities.

Last month, the Liberals presented a new defence policy aimed at giving the military the "hard power" to aggressively assert Canadian imperialist interests and ambitions around the globe. It calls for military spending to be hiked by more than 70 percent over the next decade, to $32.7 billion. This includes funds for an expanded fleet of fighter jets, 15 new warships, armed drones, and the recruitment of 5,000 additional military personnel. The new policy also says that the development of offensive cyberwar capabilities must be a top priority for the Canadian Armed Forces (CAF).

Toward this end, the defence policy paper calls for the creation of a new "Cyber Mission Assurance Program" as well as a new job category of "cyber operator" within the military in order to "significantly increase the number of military personnel dedicated to cyberwar functions." The CAF also plans to use "reservists with specialized skill-sets" to fill elements of its new cyber force.

Two weeks after the defence policy announcement, the government tabled legislation (Bill C-59) that would give the Communications Security Establishment (CSE), Canada's counterpart to the US National Security Agency (NSA), new powers to launch cyberattacks against foreign targets, including states' computer infrastructure and communications networks.

Bill C-59 is the Liberals' promised "reform" of Bill C-51, the anti-democratic law Stephen Harper's Conservative government passed in 2015 under the fraudulent pretext of fighting "terrorism." The Liberals' new legislation, however, upholds Bill C-51's main attacks on fundamental democratic rights, including granting the security agencies virtually unrestricted access to personal information collected by other government agencies.

Like Bill C-51, Bill C-59 empowers CSIS, the country's primary domestic spy service, to actively "disrupt" so-called threats to national security and, if necessary, to use illegal means to do so. And going beyond Harper's legislation, Bill C-59 expands CSIS' power to store and analyze electronic data and share it with the other spy agencies.

CSE and CSIS carry out mass surveillance operations that violate the constitutional rights of millions of Canadians and others around the world, and are implicated in conducting espionage activities against foreign countries, their leaders, opposition movements, and corporate rivals of Canadian big business.

But elements within the political establishment and the security and military apparatuses have long criticized the limited "defensive" character of the spying agency operations and called for the arming of CSE with cyber war capabilities.

Bill C-59 would enable CSE, with the approval of the ministers of defence and foreign affairs, to engage in offensive actions such as shutting down servers, planting malware on phones or other devices, and disrupting online information.

Bill C-59 also provides the legal cover for CSE to integrate its operations more closely with the Canadian military. To be sure, CSE already works closely with the CAF, Public Safety Canada, Global Affairs Canada and Shared Services Canada on cyber issues. CSE provided intelligence to the Canadian military during the Afghan war, with retired CAF head General John Adams boasting in 2010 that over half of the "actionable intelligence" that Canadian soldiers used in prosecuting the Afghan War came from the CSE.

Now, however, the spy agency will be able to wage aggressive cyberwarfare and is mandated to work with

military in waging offensive cyberwar operations.

Defence Minister Harjitt Sajjan, who expressed strong support for CSE/CAF integration, explained that “What [the section of Bill C-59 pertaining to the CSE] does…is allow the CSE to assist the Canadian Armed Forces, which was not the case before.” The new law “allows CSE to be able to (use) their specialized tools and skills to make sure…our interests are protected.”

The integration of the spying agencies with the military is part of a more aggressive, imperialist foreign policy demanded by the Canadian ruling class, which the Trudeau government is fully committed to enforcing. One day prior to Sajjan’s presentation of the new defence policy, Foreign Minister Chrystia Freeland delivered a speech in which she vowed that Canada must resort to “hard power,” i.e. war, to uphold its interests abroad. She also insisted on the maintenance of Ottawa’s strategic partnership with US imperialism, and the need for increased military spending.

One important mechanism for the expansion of joint Canada-US military-security operations will be the US National Security Agency-led “Five Eyes”, a vast spying network also involving the signal intelligence agencies of the United Kingdom, New Zealand and Australia. In fact, with its new cyber measures the Canadian state is aligning its practices with those of its partners, which are using the pretext of Russia’s and China’s development of cyberwar capabilities to dramatically increase the powers of their spy and cyber agencies.

Cyberattacks can have a devastating impact on economic and social organization. In 2010, the US, in collaboration with Israel, launched a cyberattack (using the NSA-made “Stuxnet worm”) on Iran’s nuclear enrichment plant at Natanz which forced some 1,000 centrifuges to self-destruct.

Last May, a cyber weapon concocted by the NSA was stolen and used by a group of hackers to infect some 350,000 computers. 70,000 devices such as MRI scanners, blood storage refrigerators and operating equipment used by Britain’s National Health Service were also targeted, forcing the NHS to turn away emergency room patients and divert ambulances, thus risking patients’ health and even their lives.

The Canadian ruling elite and the media have cynically welcomed the draconian Bill C-59 for its creation of a “super watch-dog” committee which will replace the Security and Intelligence Review Committee. In fact, the new National Security and Intelligence Review Agency will be staffed with tried and trusted representatives of the ruling class, and will not be accountable to the public. A National Security Commissioner will be tasked to work with the security agencies to establish legal cover for their operations, including CSIS “disruption” campaigns.

Defence Minister Sajjan acknowledged that in the case of CSE and cyberwar, details of any attack will not be made public. "Just like any other type of (military) operation, it goes through a very strict process and obviously for national security reasons, we can't outline a lot of the work that is being done" said Sajjan. A provision within Bill C-59 also states that CSE can take whatever precautions necessary to “maintain the covert nature” of its cyberattacks.