

Canada's Communications Security Establishment part of a secret state-within-the-state

Ed Patrick, Keith Jones
22 July 2013

Most Canadians had never heard of the Communications Security Establishment (CSEC), the Canadian counterpart of the US National Security Agency (NSA), prior to last month's *Globe and Mail* report that CSEC has been metadata mining Canadians' electronic communications since 2005.

And Canada's elite is determined to keep it that way—to ensure that the public knows as little as possible about the activities of CSEC.

The Conservative government and CSEC have responded with a series of lies, half-truths and disingenuous statements to the revelation that Canada's signal intelligence agency has been collecting Canadians' metadata. Peter MacKay, who until last week's cabinet shuffle was the minister in charge of CSEC, lied repeatedly and brazenly in the days following the exposure of CSEC's metadata mining, declaring that CSEC is only involved with “foreign threats.” A former CSEC deputy director, meanwhile, termed the exposure a “manufactured” story. Yet, the Supreme Court Justice who served as the government-appointed “watchdog” on CSEC's activities from August 2006 until his death in July 2009 repeatedly raised concerns that the program violated the agency's mandate and Canadians' rights.

The government's aim is to cover up the fact that the CSEC is systematically spying on Canadians and collecting information that can be—and undoubtedly is being—used by Canada's national security apparatus to identify and develop intimate portraits of the views, habits and connections of individuals and groups that it deems hostile to the interests of Canadian big business and its state.

The press and opposition parties, for their part, quickly dropped discussion of CSEC's activities.

The reality is that CSEC functions as part of a burgeoning state-within-the-state: a network of national intelligence, military and police agencies that are armed with draconian powers, subject to little and ever-shrinking judicial and

parliamentary oversight, and shielded from public scrutiny.

CSEC is, as far as we know, the most secretive part of this network. It functions under secret ministerial directives issued by the Defence Minister. Not only are the directives' contents shrouded in secrecy, even their topics are kept secret from the public, opposition and government parliamentarians, and almost all ministers.

CSEC does not report directly to parliament and its activities are not subject to the oversight of a parliamentary committee. Until 2011 it released annual reports through the Ministry of Defence that were tailored to obfuscate its activities. Since then, it is no longer obliged to publicly issue any annual report or document outlining its plans, priorities and performance.

Hugh Segal—the Conservative Senator who heads the Senate's Special Committee on Anti-Terrorism—admitted that he first learned that CSEC is metadata mining Canadians' electronic communication through the *Globe and Mail*'s June 10 report.

The government has sought to calm public concern about CSEC by claiming that it is legally barred from spying on Canadians and that there is a “legal wall” between its activities and those of the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

This is quite simply an untruth.

One of CSEC's main functions is to assist CSIS and RCMP in upholding national security.

Also, it can investigate Canadians' communications if it deems that they are relevant to any investigation it is carrying out of “foreign threats.”

Third, we now know that since 2005, and under Liberal and Conservative governments alike, CSEC has been mining the metadata of Canadians' electronic communications. The government has refused to provide any details of this program, but the US NSA—with which it has closely collaborated for more than six decades—is known to

systematically collect and analyze the metadata of all Internet, telephone and cellphone communications.

In 2007, CSEC's then head, John Adams, declared that his agency's ambition was to "master the Internet." "Our vision," Adams told the Standing Senate Committee on National Security and Defence, "is security through information superiority. We want to master the Internet. That is a challenge that no one institution—be it ours or the National Security Agency, NSA, for that matter—can manage on their own. We try to do that in conjunction with our allies."

To square their claim that CSEC is not spying on Canadians with CSEC's mining of the metadata of Canadians' electronic communications, CSEC and the government have advanced the spurious claim that metadata is "not communication" and therefore can be accessed without having to seek approval from the courts.

Significantly, the ministerial directive MacKay issued in 2011 authorizing the continuation of CSEC's metadata mining program invokes this subterfuge. According to the *Globe and Mail*, which has seen a heavily redacted version of the directive, it declares, "Metadata is information associated with a telecommunication...and not a communication."

Fourth and finally, although CSEC is legally barred from requesting its partners to spy on Canadians, nothing prohibits it and other Canadian intelligence agencies from accepting intelligence offered it by the NSA and other allied agencies. In a revealing interview with the *Toronto Star*, Wayne Easter—the minister responsible for CSIS in 2002-3—said that it was *de rigueur* for the NSA to pass on intelligence about Canadians and for CSIS to accept it. Further confirmation of this practice comes from Britain. David Blunkett, British Home Secretary from 2001-4, told that country's parliament last month that the NSA routinely "offers intelligence" to Britain's signal intelligence agency, GCHQ, so as to enable it to circumvent the restrictions on its spying on Britons without ministerial authorization.

The government and CSEC have denied that anything comparable to the NSA's PRISM program, under which the US agency has had unfettered access to the servers of major computer and Internet corporations like Apple, Google and Facebook, exists in Canada. But both the NSA and the corporations involved denied they were collaborators in any such scheme until they were unmasked thanks to the efforts of whistleblower Edward Snowden.

According to Tamir Israel, a staff lawyer with the Canadian Internet Policy and Public Interest Clinic, were Internet and phone providers being ordered by the Canadian government to provide information, the order would invariably include nondisclosure conditions.

The big corporations that control the country's telecommunications have, it should be added, a clear record of collaborating with the state. 95 percent of all requests by local police, the RCMP and CSIS for subscriber information are offered voluntarily without recourse to a warrant.

The little we do know of CSEC's activities indicates that its operations are closely integrated with those of the NSA and that the NSA views it as one its most trusted partners. CSEC, for instance, assisted the United States and Britain in spying on participants at the London G20 summit in 2009—a highly sensitive operation.

Documents leaked by Edward Snowden and published by *The Guardian* detail how CSEC, the NSA and GCHQ monitored the phone calls and computer usage of foreign politicians and officials, including those of NATO allies such as France and Germany.

CSEC is also deeply involved in the Canadian elite's predatory wars. In 2010, the then CSEC chief, retired CAF General John Adams, boasted, "If you were to ask the Canadian Forces if there is anyone that has saved Canadian lives in Afghanistan, they would point to us." He claimed that over half of the "actionable intelligence" that Canadian soldiers use in prosecuting the Afghan War came from CSEC.

As around the world, the Canadian elite has used the bogus "war on terror" to justify an assault on democratic rights and to develop the veritable infrastructure for a police state. CSEC has been front and center in these developments. First Liberal and now Conservative governments have lavished resources on it. CSEC's staff has doubled in the past decade and now numbers more than 2,000, while its annual budget has mushroomed to about \$400 million.

Currently under construction is a new nearly \$1 billion headquarters. The enormous new CSEC complex will be located next to CSIS's headquarters. That a bridge is being built between the two headquarters further underlines the close working relationship between the two spying agencies and puts the lie to the government's claim that "legal" walls separate their operations and confine them to distinct domains.



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact