An excerpt of CSE's response to CBC's questions

Friday, March 6, 2015
CSE response:

Here is CSE's official response to this set of questions.

- CSE has the authority under the National Defence Act to acquire and use information from the global information infrastructure to collect foreign signals intelligence. This protects Canadians, Canada and our allies.

- Under this foreign intelligence mandate, CSE does not direct its foreign signals intelligence activities at Canadians or anywhere in Canada.

- Under its cyber-security mandate, CSE monitors government networks with the sole purpose of protecting them from malicious cyber activity.

- CSE's foreign signals intelligence has played a vital role in uncovering foreign-based extremists' efforts to attract, radicalize, and train individuals to carry out attacks in Canada and abroad.

- Any suggestion that CSE monitors Canadian internet space – outside of the Government of Canada network – for any purposes other than those defined in the National Defence Act is false.

- CSE regrets the disclosures, and the speculative and often incorrect analysis of them, particularly given that the professional and dedicated men and women of CSE work diligently every day to protect Canadians.

- The independent CSE Commissioner scrutinizes CSE's activities. The CSE Commissioner has never found CSE to have acted unlawfully, and has noted CSE's respect for the privacy of Canadians.

Monday, March 2, 2015
CSE response:

Many of the questions presented relate to specific operations, methods or capabilities that help protect Canada and Canadians against threats. As you know, CSE must respect the *Security of Information Act* and cannot comment on classified operations, methods and capabilities. In some instances, the questions presented indicate a misunderstanding of CSE's actual capabilities or intentions. Furthermore, CSE regrets that the publication of these documents renders our methods less effective when addressing threats to Canada and Canadians.

The leaked materials are dated documents, and some explored possible ideas to better protect the Government of Canada's information systems while also seeking cost efficiencies. As a result, information in these documents does not necessarily reflect current CSE practices or programs, or the degree to which CSE has visibility into global or Canadian infrastructures.

In moving from ideas or concepts to planning and implementation, we examine proposals closely to ensure that they comply with the law and internal policies, and that they ultimately lead to effective and efficient ways to protect Canada and Canadians against threats.

Technologies or tools that are deployed or used by both operational areas are done so separately under CSE's foreign intelligence or cyber defence mandates, and information is managed separately in compliance with a suite of internal policies specific to each mandate.

Under its IT security mandate, CSE has in place automated scanning on government networks to identify malicious cyber activity. CSE only collects information that is necessary and relevant to understand the nature and methods of malicious cyber threats and to prevent malicious cyber activity against Government of Canada systems and networks.

When information is shared between the two operational areas, it is to help better understand malicious cyber threats so that CSE can more effectively defend government systems. For example, where appropriate, information about foreign cyber activities discovered by our IT security analysts can be shared with designated foreign signals intelligence analysts for follow-up under CSE's foreign intelligence mandate. Foreign intelligence on these threat activities, and the methods and techniques behind them, is critical to understanding, mitigating and defending against malicious cyber activities that threaten Canadian infrastructures and information.

Information collected by CSE is managed according to established data retention schedules that are documented in internal policies and procedures. To provide more detail could assist adversaries who want to conduct malicious cyber activity against government networks, or evade our foreign signals intelligence efforts.

Under its assistance mandate, CSE provides technical assistance to federal law enforcement and security agencies only at their specific request, and only under the requesting agency's legal authority, such as a warrant.

Privacy protections are established by law and reflected in policies governing CSE's activities. Measures are built into CSE's operations and technologies for the handling, retention, use and destruction of information about Canadians.

The independent CSE Commissioner and his staff scrutinize CSE activities. The CSE Commissioner has never found CSE to have acted unlawfully, and has noted CSE's respect for the privacy of Canadians.

Tuesday, March 3, 2015
CBC questions:

1. We understand CSE employees are bound by secrecy under SIA due to national security concerns. But why can't the agency disclose whether it monitors all of Canadian internet traffic?
(Such a revelation doesn't put national security in danger and is in the public's interest.)

2. In which instances do our questions (sent February 24, 2015) "indicate a misunderstanding of CSE's actual cyber capabilities or intentions?"

Please know, based on CSE's own documents, and in consultation with numerous authorities across a spectrum of view points and expertise, CBC is preparing to report the following:

CSE has developed sophisticated capabilities to exploit cyber networks, as well as to attack and disrupt potential opponents/threats.
These CNE/CNA capabilities, and Canada's global access points and sensors are the very tools CSE could use to assist other agencies (CSIS, RCMP) to 'disrupt' terror threats should Bill C51 become law.

Please answer each of the following:

3. What of the above statement (*in italics*) is incorrect?

4. You indicated to CBC in your responses of March 2 that CSE's leaked documents are both dated, and spoke of "plans" and that "as a result, information in these documents does not necessarily reflect current CSE practices or programs, or the degree to which CSE has visibility into global or Canadian infrastructures."

However, the 2011 CASCADE document discusses plans for 2015 and states that CSE currently has "full visibility of our national infrastructure."
Are you saying CSE no longer has 'full visibility' of Canadian cyber infrastructure?

5. Under what authority is CSE currently monitoring Canada's entire national cyber infrastructure?

6. On which dates has a minister's of defence authorized monitoring of the entire national cyber infrastructure under Mandate A?

7. (above) Under Mandate B?

Tuesday, Feb. 24, 2015
CBC questions:

1. Is CSE monitoring all of Canada's internet space?
2. If so, under what mandates (A/B or C)?
3. Is CSE collecting data or metadata from Canada's entire internet space?
4. How much of this collection is used and retained?
5. For how long?
6. Has CSE succeeded in merging its Cyber Sensor Architecture (both defence of Canadian government networks using Photonic Prism program, and foreign/warrants intelligence gathering through the EONBLUIE program) as imagined as a goal for 2015 in the CSE slidedeck "CASCADE?"
7. What does it mean for Photonic Prism and EONBLUE sensors to be merged?
8. What is the name of the newly unified sensor architecture program that has replaced/merged these two previous systems?
9. What does it mean that CSE has "full visibility of our national infrastructure?" (CASCADE slide deck, p. 30)
10. What are the "Special Sources" (which telecommunications companies, internet cables, core internet providers?) that provide CSE with a view of all of Canadian Internet Space? (CASCADE slide deck,
illustration p 19)?
11. Under what authority is CSE acquiring access to all 'international gateways accessible from Canada" from these so called "Special Sources?" (CASCADE slide deck p. 22)
12. How, under the newly 'synchronized' system employing 'common data repositories,' does CSE distinguish and keep separate (both in CSE use and in sharing with allies) the data collected its two separate mandates? (Canadians emails and data collected expressly under the "cyber security mandate" to protect government networks, versus data/metadata collected under the 'foreign intelligence" and/or 'assistance' to CSIS/RCMP/ect 'SIGINT" mandate?) (CASCADE slide deck p.23).
13. How is surveilling the entire internet 'national infrastructure' effective in defending against cyber attacks?
14. In the 2010 slide deck "CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach" there is a diagram on page 15, laying out the various types of internet traffic/communications being collected and observed by CSE under its different mandates (Mandate B - defence of government networks, versus Mandates A + C - foreign intelligence gathering, and assistance to CSIS/RCMP/etc).

How do you account for the "domestic to domestic" communication that CSE is surveilling under its Mandate A + C ...distinct from the 'warranted domestic' collection identified in the

diagram? (CSE isn't supposed to be targeting/directing activities at Canadians, beyond warranted authorization). Can you explain this ?

15. On page 22 of the 2010 slide deck "CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach" there is a chart on "Cyber Activity Spectrum" which details CSE's capacity for Cyber Network Exploitation and Attacks (implants, taking control, disruption, destroying of adversary networks). Can you provide examples when these capabilities have been used?
16. Under what authority does CSE break into, disrupt or destroy adversary infrastructure?
17. How many times since 2010 has CSE been called on under its Mandate C (Assistance) to employ these CNE/CNA capabilities?
18. How would Bill C-51, should it become law, affect CSE's activities in the CNE/CNA realm?