Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

FEB 0 6 2018

Our file Notre référence
A-2017-00073

Mr. Colin Freeze
The Globe and Mail
351 King Street East, Suite 1600
Toronto, Ontario M5A 0N1

Dear Mr. Freeze:

This is further to your request submitted under the *Access to Information Act* received on November 7, 2017 for:

"The current Bill C-59 makes certain changes to how CSE could help enforce the Investment Canada Act's national-security review provisions. Please release any briefing notes, bulletins, studies, media lines and PowerPoint decks from the 2017 calendar year speaking to why these fixes are necessary and what roles and responsibilities at CSE may change. Also please include any email correspondence Greta Bossenmaier or her designates may have had with Public Safety Canada officials on this subject matter in January, 2017 and March 2017. "

Enclosed please find all requested records that could be located using the Department's best efforts, within the restraints of the *Act.* You will notice that certain information has been withheld from disclosure pursuant to section(s) 15(1) - DEF Defence of Canada, 19(1) personal information, 21(1)(a) advice or recommendations, 21(1)(b) consultations or deliberations, 69(1)(a) proposals or recommendations to Council, and 69(1)(g) re (f) Any records making a reference to (f) of the *Act.*

Please be advised that you are entitled to file a complaint with the Office of the Information Commissioner concerning the processing of your request within sixty days of the receipt of this notice. In the event that you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Should you require any additional information or assistance regarding this request, please contact the CSE ATIP Unit at (613) 991-8443.

Yours sincerely,

Dominic Rochon
Access to Information and Privacy Coordinator

Enclosure: 15 pages

Canada

15(1) - DEF DEFENCE OF CANADA
information the disclosure of which could reasonably be expected to be injurious to the conduct of the defence of Canada or any state allied or associated with Canada

---

19(1) PERSONAL INFORMATION
Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in section 3 of the Privacy Act.
(2) The head of a government institution may disclose any record requested under this Act that contains personal information if
(a) the individual to whom it relates consents to the disclosure;
(b) the information is publicly available; or
(c) the disclosure is in accordance with section 8 of the Privacy Act.

21(1)(a) ADVICE OR RECOMMENDATIONS
advice or recommendations developed by or for a government institution or a minister of the Crown,

---

21(1)(b) CONSULTATIONS OR DELIBERATIONS
an account of consultations or deliberations involving officers or employees of a government institution, a minister of the Crown or the staff of a minister of the Crown,

---

69(1)(a) PROPOSALS OR RECOMMENDATIONS TO COUNCIL
memoranda the purpose of which is to present proposals or recommendations to Council;

69(1)(g) re (f) ANY RECORDS MAKING A REFERENCE TO (F)
Records that contain information about the contents of any record within a class of records referred to in paragraphs (f).

Pages 1 to / à 39

are duplicates

sont des duplicatas

Pages 40 to / à 82

are duplicates

sont des duplicatas

Examples of *CSE Act* Concepts

New Foreign Signals Intelligence Tools

- CSE could gather information that provides an advantage to military commanders leading CAF missions and other Canadian officials charged with mitigating threats to terrorism, espionage, kidnapping and cyber intrusions.

Protective Services for Non-GoC Clients

- CSE could more extensively share information about specific cyber threats with the owners of critical infrastructure, like telecommunications companies or the banking sector.

- CSE would also be permitted to deploy its unique cybersecurity tools on non-government systems at the request of the owners of those systems.

Defensive Active Cyber Operations

- CSE disables a foreign server attempting to steal information from the Government of Canada.

- CSE could shut down a foreign web server launching malicious cyber operations against critical infrastructure.

- CSE could corrupt information sitting on foreign servers that was stolen from a Government of Canada network.

Active Cyber Operations

- CSE could use online capabilities to interfere with terrorist attack plans.

Assistance to DND/CAF

- CSE could use advanced techniques to disrupt adversaries' ability to communicate with each other.

Assistance (more broadly):

- CSE currently assists federal law enforcement and security agencies in various ways, such as collecting and processing communications, providing linguistic support, or designing technical solutions.

- For example, CSE could decrypt encrypted data to assist CSIS or RCMP in an investigation.

Publicly Available Information:

- CSE could, for example, use publicly available information acquired from social media to contribute to a report on a foreign country, if the information is foreign intelligence value.

- CSE could also conduct research on social media to assess morale of foreign fighters abroad. CSE would not be interested in the identities of the individual on the platform, but rather the information they are posting.

- CSE could conduct basic internet research and, for example, download and read cybersecurity papers written by Canadian authors.

Infrastructure Information:

- This provision would allow CSE to undertake research and development, to test a system, or to conduct cybersecurity and information assurance activities on the infrastructure from which the information was acquired.

Testing and Evaluation of Products:

- CSE may test a product prior to the product being used by the Government of Canada.

- CSE may test a system for vulnerabilities for the purpose of providing advice or guidance to Canadians under the cybersecurity and information assurance aspect of CSE's mandate.

***Investment Canada Act*:**

- This provision will allow CSE to leverage its expertise to support the review of foreign investments in Canada, particularly on investments in the information and communications technologies sector, by providing analysis on information already in CSE's possession.

Cybersecurity and Information Assurance

- CSE may carry out activities on information infrastructures to identify and isolate malicious software, prevent malicious software from harming those information infrastructures or mitigate any harm that malicious software causes to them.

- This subsection will also allow CSE to analyse information in order to be able to provide advice on the integrity of supply chains and on the trustworthiness of telecommunications, equipment, and services.

CSE's Activities

Under the *CSE Act*, CSE's activities are subject to two important restrictions:

- Activities carried out by CSE in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada (subsection 23(1)).
- Activities carried out by the Establishment in furtherance of the defensive cyber operations or active cyber operations aspect of its mandate (a) must not be directed at any portion of the global information infrastructure in Canada; and (b) must not be carried out except under an authorization (subsection 23(2)).

The *CSE Act* permits CSE to undertake specific activities in its furtherance of its mandate despite the restrictions in 23(1) and (2). These activities are listed in section 24.

Publicly Available Information

Publicly available information is information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or is available to the public on request, by subscription, or purchase.

Paragraph 24(1)(a) states that CSE may acquire, use, analyse, retain, or disclose publicly available information. CSE could only carry out these activities in support of its mandate. For example, CSE may use publicly available information from social media to contribute to a report on a foreign country, if the information is of foreign intelligence value.

For example, CSE may use publicly available information in order to help protect the privacy of Canadians. Publicly available information may be used, as part of a larger analysis, in order to assess the nationality of a corporation or individual. This is done to minimize privacy risk by limiting the incidental collection of information relating to Canadians and persons in Canada under the foreign intelligence or cybersecurity aspects of CSE's mandate. Being able to assess the nationality of an entity allows CSE to establish terms and criteria that will identify information of *foreign* intelligence value, for the purposes of CSE's foreign intelligence mandate, and will help CSE to limit the incidental collection of information relating to Canadians and persons in Canada, as well as to apply measures to protect their privacy, under both mandates.

The acquisition and use of information already in the public realm would generally not intrude upon protected privacy rights. Where it would, the reasonable expectation of privacy would generally be low because the information is publicly available. Nevertheless, CSE must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention, and disclosure of publicly available information.

CSE may undertake these activities despite subsections 23(1) and (2).

Infrastructure Information

Infrastructure information means any information relating to (a) any function component, physical or logical, of the global information infrastructure; or any events that occur during the interaction between two or more devices that provide services on a network – not including end-point devices that are linked to individual users – or between an individual and a machine, if the interaction is about only a functional component of the global information infrastructure. Infrastructure information excludes information that could be linked to an identifiable person.

Paragraph 24(1)(b) states that CSE may acquire, use, analyse, retain, or disclose infrastructure information. CSE could only carry out these activities in support of its mandate. For example, this provision would allow CSE to undertake research and development, to test a system, or to conduct cybersecurity and information assurance activities on the infrastructure from which the information was acquired.

CSE may undertake these activities despite subsections 23(1) and (2).

Testing and Evaluation of Products

Paragraph 24(1)(c) would allow CSE to test or evaluate products, software and systems, including testing or evaluating them for vulnerabilities. For example, CSE may test a product prior to the product being used by the Government of Canada, or CSE may test a system for vulnerabilities for the purpose of providing advice or guidance to Canadians under the cybersecurity and information assurance aspect of CSE's mandate.

CSE may undertake these activities despite subsections 23(1) and (2).

Investment Canada Act

As a prescribed investigative body under the *National Security Review of Investment Regulations,* CSE contributes to the review, under the *Investment Canada Act* (ICA), of proposed foreign investments in Canada that may be injurious to Canada's national security. In this role, CSE provides advice to the Minister of Public Safety and Emergency Preparedness and to the Minister responsible for the administration of the ICA.

Subsection 24(2) would allow CSE to analyse information for the purposes of its role under the ICA. This provision will allow CSE to leverage its expertise to support the review of foreign investments in Canada, particularly on investments in the information and communications technologies sector, by providing analysis on information already in CSE's possession.

CSE may undertake these activities despite subsection 23(1).

Cybersecurity and Information Assurance

Subsection 24(3) outlines activities that CSE may undertake in furtherance of the cybersecurity and information assurance aspect of its mandate.

First, CSE may carry out activities on information infrastructures to identify and isolate malicious software, prevent malicious software from harming those information infrastructures, or mitigate any harm that malicious software causes to them. To be clear, the proposed *CSE Act* does not give CSE the ability to evaluate *any* system for vulnerabilities. The legislation sets out a clear process that must be followed in order for CSE to deploy its cybersecurity tools on federal government and non-federal government systems.

Further, this subsection will also allow CSE to analyse information in order to be able to provide advice on the integrity of supply chains and on the trustworthiness of telecommunications, equipment, and services.

CSE may undertake these activities despite subsection 23(1).

From:
Sent: September-29-17 10:13 AM
To:
Subject: FW: Summary - Briefing to Academics September 27

Classification: UNCLASSIFIED

From: Rochon, Dominic J
Sent: September-29-17 8:27 AM
To: excom_dist
Cc: Millar, Scott D; Williams, Christopher R;
Subject: FW: Summary - Briefing to Academics September 27

Classification: UNCLASSIFIED

Haven't had a chance to debrief everyone on the wonderful events of this week surrounding Bill C-59... but seeing as how the goal is really to simply attend, make sure nothing blows up, and (provided nothing blows up) immediately forget the event ever happened and move on to the next one, the bottom line is ALL went well Tuesday, Wednesday and Thursday... so let's bring on Friday.

For those who have time, and a little more curiosity, you will find below an account of the academic briefing from Wednesday morning (the 90 minute portion allocated to the CSE Act). Scott Millar, and I provided answers. What the account below does not say is that never got a chance to speak, so I promised to get back to him with some observations to the various questions he posed I just sent those answers and will share with you on other system.

Happy to address any questions or concerns if you have any.

Dom

s.21(1)(a)
s.21(1)(b)

From:
Sent: September-27-17 3:10 PM

UNCLASSIFIED

To: Rochon, Dominic J
Cc: Millar, Scott D;
Subject: Summary - Briefing to Academics September 27

Classification: UNCLASSIFIED

Dominic – summary based on my notes, for you to provide to the Chief and/or others. If anything doesn't make sense, let me know.

Please find below highlights from today's briefing to academics. Deputy Chief Policy and Communications (Dominic Rochon) and Director General Strategic Policy and Planning (Scott Millar), with support from Strategic Policy (provided the brief. Part one of this brief was focused on CSE, while the second was focused on CSIS.

Overall, the meeting went very well. Attendance by academics included:

and

and participated on the phone.

Questions to CSE included:

- **Q.** - If the aim of the Intelligence Commissioner is to respond to the concerns raised in the BCCLA case, the Act should include among the "triggers" for the Intelligence Commissioner's approval, then is just contravening an Act of Parliament broad enough? Should there be another "trigger" for when CSE's activities may not violate a law, but may have Charter concerns?
    - **A. CSE** - BCCLA still studying the Bill to decide what course of action to take. The CSE Act brings metadata into the MA regime. This expands on the focus of the NDA (private communications). CSE is bound by the Charter, as are all departments, and if we are in potential contravention of the Charter, the expectation is that we would week an MA.
    - **Follow-up by** - Notes that it seems he and CSE don't have opposite views on the issue of getting an authorization if there are Charter implications, but suggested that this might need a frank acknowledgement in the bill.
- **Q.** - Is the "trigger" for an authorization in the foreign intelligence mandate only when CSE is acquiring information? Does it apply to everything done in advance of acquiring the information? (ie. if you place an implant on a network, but it is not collecting information, does the MA still cover this activity).
    - **A. CSE** - The MA covers everything that leads up to interception. It covers the whole process, as well as the use, analyse and retention of the information.
- **Q.** - How is "directed at" interpreted in regards to 24(4)?
    - **A. CSE** - OCSEC has been reviewing CSE for a very long time, and we have been using the concept of "directed at" since the NDA legislated its authorities. OCSEC has never recommended that this term be defined.
    - **Follow-up by** - adding the word "only" into 24(4) would solve his "trigger" issue referenced in Question 1. Suggested it read: "The Establishment may only acquire information relating to a Canadian ... in the course of carrying out activities under an authorization..."

- **Q.** - Could incidental collection happen that didn't violate a law or trigger the Charter?
    - **A. CSE –** No, this always has Charter engagement and for that reason CSE would get an authorisation. The authorization regime and the Intelligence Commissioner's approval of the authorizations is meant to mitigate this risk.

- **Comment -** made some preliminary comments about how the legislation fails to properly introduce Canadians to the complex principles of CSE. The Act fails to put into words the principles that made the Act necessary – it needs to be rewritten to put the principles/value statement at the start.
    - **A. CSE –** Bill is not a communications product. Drafting legislation is not concerned with communications issues, but with legal conventions.

- **Q.** - Why is there no clear distinction between cybersecurity and defensive cyber operations?
    - **A. CSE –** There are clear distinctions between these mandates in the Act. DCO is about taking action online, outside of Canada, to prevent or stop acts threatening Canadian infrastructures.

- **Q.** - There is a collision between two descriptions in the cybersecurity mandate in 23(2)(a) (no activities directed at the GII in Canada for ACO and DCO) and 24(1)(b) (infrastructure information carve out)?
    - **A. CSE –** Section 24 is the carve out sections of the CSE Act and are not subject to restrictions in section 23. Pointed to the word "despite" in Subsection 24(1) lead in.

- **Q.** – It is not clear how big of a deal the Investment Canada Act is to CSE. Does this a green-light for CSE to engage in the acquisition of information on Canadians for ICA purposes?
    - **A. CSE –** The intent of this provision is not the foreign intelligence mandate, but rather the cybersecurity mandate. This does not allow CSE to acquire information, but rather to analyze information.

- **Q.** – When would CSE not need an MA? Is it clear to Canadians?
    - **A. CSE –** MA's are at the core of CSE's business and cover everything that CSE does.

- **Q.** · Is the CSE Act about ensuring CSE can engage in bulk/mass surveillance? If it is, then say yes (it appears so because of unselected information). If not, is there a way of saying no in the Act and clarifying CSE's primary mission?
    - **A. CSE –** CSE may only undertake activities that are in support of the intelligence priorities.

- **Q.** - Why is the role of the Intelligence Commissioner limited to only certain authorizations? Does the decision to give the Intelligence Commissioner an approval/oversight function take away from Ministerial accountability?
    - **Follow-up by** - The Intelligence Commissioner's role is necessary to solve Charter issues. CSE needs to add this level of oversight – it is a necessary provision.
    - **A. CSE -** Yes, the Intelligence Commissioner's role is limited to the specific authorizations. These authorizations are the ones where there will be acquisition of information. No information is acquired

under DCO and ACO authorizations. Further, there are options to extend the authorizations if the Minister and Intelligence Commissioner can't agree.

  - **A. Public Safety** – Further, the Intelligence Commissioner is reviewing the conclusions of the decision-maker (ie. was the decision-maker given adequate information and would a reasonable person come to the same conclusion given the information they have). The Minister maintains control.

- **Q.** – Should the prohibited conduct laid out in section 33 also apply to the foreign intelligence mandate? As this mandate now includes the ability to "disrupt" a system, this could have downstream effects. Further, why is the list shorter than what is in CSIS's Act?

  - **A. CSE** - We hear the point about meshing with the prohibited conduct in CSIS's Act and expect that this will be raised in Committee. Note that the authorizations also have a proportionality provision and that all these activities will be subject to review.

  - **Follow-up by** – Is there prohibited conduct laid out in the Acts of our Allies?

    - **A. CSE** - Not sure this explicit in legislation of our allies. We'd need to check on that.

- **Q.** – While this does a lot of the transparency and accountability of CSE, there is little to no opportunity for external experts to review the work of the legislated review bodies. This is something done by our allies, specifically by the US.

  - **A. CSE** - There is a Transparency Charter coming, an initiative by the Minister of Public Safety, which might respond to some of these concerns.

- **Comment -** The scope of publicly available information needs to be clarified, as well as the protections afforded to Canadians. As well, there is ongoing lack of clarity on how CSE provides assistance to other departments. It makes sense for CSE to do this, but it would be helpful to have more clarity about how it is done.

- **Q.** – What does the process for vulnerabilities/equities look like? Clarity on this would be helpful.

  - **A. CSE** - CSE has a rigorous process in place to review and access vulnerabilities. It takes a security-first focus.

- **Q.** – In the US, Cyber Command is a separate entity. Why is everything housed together at CSE?

  - **A. CSE** - We model ourselves more after GCHQ and ASD, who are similar in size to us than the US's community. We partner with DND, but we have our own DM and do not report to CDS. Further, when the Defence Policy Review, released earlier this Spring, and it said that a modern military needed to have these cyber capabilities, it was decided that to leverage CSE rather than duplicate capabilities.

No questions/comments came from or

If you have any questions, please don't hesitate to ask.

Cheers,

Strategic Policy

From:
Sent: September-27-17 9:51 PM
To:
Cc:
Subject: FW: Summary - Briefing to Academics September 27

Classification: UNCLASSIFIED

Thought you might be interested in summary of today's session.

Highlighted a part you might like ;)

Also, on the ICA part I made sure that Scott said that that provision in the Act only related to analysis.

From:
Sent: September-27-17 3:10 PM
To: Rochon, Dominic J
Cc: Millar, Scott D;
Subject: Summary - Briefing to Academics September 27

Classification: UNCLASSIFIED

Dominic – summary based on my notes, for you to provide to the Chief and/or others. If anything doesn't make sense, let me know.

Please find below highlights from today's briefing to academics. Deputy Chief Policy and Communications (Dominic Rochon) and Director General Strategic Policy and Planning (Scott Millar), with support from Strategic Policy (provided the brief. Part one of this brief was focused on CSE, while the second was focused on CSIS.

Overall, the meeting went very well. Attendance by academics included:

and

and participated on the phone.

Questions to CSE included:

- **Q.** - If the aim of the Intelligence Commissioner is to respond to the concerns raised in the BCCLA case, the Act should include among the "triggers" for the Intelligence Commissioner's approval, then is just contravening an Act of Parliament broad enough? Should there be another "trigger" for when CSE's activities may not violate a law, but may have Charter concerns?
    - **A. CSE -** BCCLA still studying the Bill to decide what course of action to take. The CSE Act brings metadata into the MA regime. This expands on the focus of the NDA (private communications). CSE is bound by the Charter, as are all departments, and if we are in potential contravention of the Charter, the expectation is that we would week an MA.

Pages 93 to / à 95

are duplicates

sont des duplicatas

Pages 96 to / à 99

are duplicates

sont des duplicatas

Pages 100 to / à 103

are duplicates

sont des duplicatas

From:
Sent: July-25-17 2:46 PM
To:
Cc:
Subject: ICA in the CSE Act

Classification: UNCLASSIFIED//CSE OFFICIAL USE ONLY

Hi

There has been nothing said publicly on the ICA yet. There isn't anything in the Charter statement or on our website. We have nothing in our Q&As we did for Cabinet/Tabling Day on this topic, nor has it been referenced in any of the media monitoring has pulled together.

What we do have is the following from an issue note on ICA developed for Main Estimates:

Investment Canada Act (ICA)

- In 2009, Canada introduced national security review provisions to the ICA, which fall to the purview of the Minister of Public Safety, who, as required, advises the Minister of Innovation, Science, and Economic Development Canada on such issues.
- The provisions permit the review of proposed foreign investments in Canada that may be injurious to Canada's national security.
- Investments where the enterprise value of the assets of the Canadian business exceeds prescribed monetary thresholds, or those raising national security concerns, are subject to government approval.
- The provisions cover all foreign investments captured under the ICA.
- Public Safety Canada is the lead responsible for identifying national security concerns posed by these investments.
- CSE, as a prescribed investigative body under the ICA, contributes to these reviews as necessary in its areas of expertise.

This is out of the draft clause-by-clause:

SUBSECTION 24(2): *Investment Canada Act*
Analysis

Subsection 24(2) makes it explicit that CSE's analysis of information for purposes of providing advice under the *Investment Canada Act* is not subject to the prohibition of directing activities at Canadians or persons in Canada.

CSE, as a prescribed investigative body under the *Investment Canada Act*, contributes to the review of proposed foreign investments in Canada that may be injurious to Canada's national security, as necessary in its areas of expertise (information and communications technology). In this role, CSE

provides advice to the Minister of Public Safety and Emergency Preparedness and to the Minister responsible for the administration of the *Investment Canada Act*. Importantly, this section only applies to analysis of information not the acquisition of information.

Let me know if you need anything else.

Page 106

is withheld pursuant to sections

est retenue en vertu des articles

69(1)(a), 69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 107 to / à 149
are withheld pursuant to sections
sont retenues en vertu des articles

69(1)(a), 69(1)(g) re (f)

of the Access to Information
de la Loi sur l'accès à l'information

Page 150

is withheld pursuant to sections

est retenue en vertu des articles

69(1)(a), 69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 151 to / à 189
are withheld pursuant to sections
sont retenues en vertu des articles

69(1)(a), 69(1)(g) re (f)

of the Access to Information
de la Loi sur l'accès à l'information

Pages 190 to / à 193

are duplicates

sont des duplicatas

Pages 194 to / à 197

are duplicates

sont des duplicatas

Pages 198 to / à 201

are duplicates

sont des duplicatas

UNCLASSIFIED

Communications Security Establishment | Centre de la sécurité des télécommunications

MEDIA RESPONSE LINES/RÉPONSE AUX MÉDIAS

ISSUE/ENJEU: Proposed CSE Act (Bill C-59) / Investment Canada Act

Media Query/Demande:

Date: 26 July 2017

Due: 26 July 2017

OVERVIEW/APERCU

A national security reporter from contacted the Minister's Office with specific questions about CSE activities related to the *Investment Canada Act.* An initial question was answered by the Minister's Office and a more detailed follow up was forwarded to CSE for response.

QUESTIONS AND ANSWERS

From reporter via MNDO:

I'm unaware of the precise legalities that would currently allow CSE to legally direct its machinery at Canadians so as to advance the aims of the investment Canada Act.

Is this currently being done under some sort of executive authority (ie a ministerial directive or authorization?)

Or is it some sort of warranted "section C" assistance power done in conjunction with another federal agency (such as, potentially, CSIS)?

Either way why would CSE need an explicit standalone statutory power to accomplish what is already being done via other means ?

Direct questions to CSE

1. First off, CSE appears is getting some sort of legislated power to ***warrantlessly spy*** (to some degree or another) on Canadians in this realm under the say-so of its own senior officials (i.e. not ministers, not judges). CSE has no analogous authorities to do similar things under any other law, so far as I am aware.

2. This also risks being construed as an explicit end run around the judicial branch of government, which referees CSE assistance to other federal entities in other partnerships. (i.e. Consider how unrelated CSE-enabled "DIFT" investigations are now sparked via Section 21 CSIS warrants. In fact, it is possible that Investment Canada Act reviews are currently being accomplished under similar CSE arrangements with CSIS now. Difference being, Federal Court judges would ultimately green light or red light such activities,)

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

3. Much rides, however, on what exactly is meant in C-59 by ***analyse information*** and whether it is akin to what I just called ***warrantless spying.*** For that distinction to be clearer you would need to know : Whose information? Where from? What kind? And does it follow then, that CSE may be getting new powers to ***acquire*** (within Canada) so it can fulfill its legal mandate to ***analyse*** it ?

All that said, I have an inferential inkling of what problem this may be meant to fix.

Under the Investment Canada Act the ministers appear to be given broad authorities to request, compel or otherwise acquire records relating to corporations whose acquisition by foreigners would trigger natsec concerns.

Yet the ministers would not themselves have the expertise or capacity to followup by putting those piles of records into any perspective, for example by "contact chaining" out significant phone numbers or IP addresses, and putting them into a global context, thereby seeing whether any adversaries turn up.

Only CSE could do that. Yet the ministers might not be able to make a direct approach to CSE for help because under its mentions only "federal law enforcement and security agencies." This may be an important legal distinction because its unclear to me what status any outside Minister might have to get CSE's assistance.

Plus in any contact-chaining exercise the ministers might spark could into the inevitable "minimization" procedures CSE would apply by default to any Canadian citizens or based-in-Canada entities who turned up in the chain. Which would defeat the point of the whole natsec review, especially if the ministers' ability to override the minimization was in question

Response

We're happy to help point you in the right direction as you continue your summer legislative reading. I hope this helps set things straight and will assure you that there are "end-runs" or "warrantless spying" provisions hiding in the proposed C-59:

As CSE is prohibited from directing its foreign signals intelligence activities at Canadians located anywhere or any person in Canada, the foreign intelligence that CSE provides for the administration of the ICA is not acquired from foreign intelligence activities directed at Canadians or any person in Canada. The inclusion of the clause you referred to in the CSE Act is to increase clarity and transparency of CSE's authority to analyze (not acquire) information relating to specific ICA transactions. One of the key expected outcomes of C-59, and the CSE Act specifically, is to increase clarity and understanding of CSE's authorities and activities. Currently, pursuant to the National

Canada

Communications Security Establishment | Centre de la sécurité des télécommunications

Defence Act, CSE provides foreign intelligence, again not directed at Canadians or anyone in Canada, to support the ministers responsible for the administration of the ICA. The proposed legislation provides this clarity. As you know, CSE has unique knowledge and expertise of information and communication technologies and may be called upon to provide advice to the Government when requested. In addition, OCSEC reviews all CSE activities, including those related to the ICA. The proposed bill also ensures that all CSE activities will be subject to the proposed enhanced accountability measures contained in the Bill.

Please let us know if you have any further questions.

With regards to the BG briefing you have requested, we're a bit thin on the ground this week, but we will see if we can look to set something up for next week.

Original Questions to MND:

Re: C-59 Wondering whether the government has ever fully articulated the carve-out regarding CSE powers and the Investment Canada Act. (see below)

i.e. Are you aware whether there are any materials published to date that explain the rationale ?

Whether this amounts to a break from past practices?

What specifically is meant by "analyze information" ? (i.e. Does this include collecting new information? Or what kinds of preexisting information would be analyzed? Etc.)

(2) Despite subsection 23(1) [*a provision barring CSE from directing its activities at Canadians*] in furtherance of its mandate the Establishment may analyse information for the purpose of providing advice to the Minister of Public Safety and Emergency Preparedness and to the Minister responsible for the administration of the *Investment Canada Act* with regard to that latter Minister's powers and duties under Part IV.1 of that Act. [to order a review of foreign investments for national security reasons]

MND Response (Press Sec)

I'm told that this clause makes explicit CSE's existing role in support of reviews under the ICA. It doesn't represent a new authority (although C-59 does propose significant and increased accountability measures), or permit CSE to direct its foreign signals activities at Canadians or anyone in Canada.

Canada