CBC Radio-Canada

DEAN BEEBY <dean.beeby@cbc.ca>

CSE monitoring at a Canadian airport

1 message

DEAN BEEBY <dean.beeby@cbc.ca> Wed, Feb 18, 2015 at 5:08 PM
To: Robert Russo <rob.russo@cbc.ca>, Allison Brachman <allison.brachman@cbc.ca>, Nick Gamache <nick.gamache@radio-canada.ca>, Heather Spiller <heather.spiller@cbc.ca>, Chris Carter <chris.carter@cbc.ca>
Cc: me@valerieboyer.net

CSE today delivered an access-to-information package in response to a request from Valerie Boyer for briefing material related to the Jan. 30, 2014, CBC story based on a Snowden document, which was a slide deck from 2012. The online piece was co-written by Greg Weston, Glenn Greenwald and Ryan Gallagher, and revealed a SIGINT operation at an unidentified Canadian airport to monitor IP addresses.

The heavily censored package has no particular bombshells that I can see, though there are tidbits. It contains a slide-by-slide critique of how the Snowden document reveals tradecraft to potential targets, for example.

Someone better versed in this story than I should review these several dozen pages.

Dean Beeby, Senior Reporter
CBC Ottawa Parliamentary Bureau
613.288.6945 / c 613.297.8540
Twitter @DeanBeeby
dean.beeby@cbc.ca
www.cbc.ca

s.15(1) - DEF

[redacted]

From: [redacted]
Sent: April-30-14 10:35 AM
To: [redacted]
Cc:
Subject: FW: IP Profiling Metadata Analysis Sample - Summary

Importance: High

Classification: CONFIDENTIAL//SI

Gentlemen,

The summary.

Cheers.

[redacted]

CSE/CST
SLT/[redacted]
[redacted]

From: [redacted]
Sent: April-30-14 10:34 AM
To: [redacted]
Cc:
Subject: IP Profiling Metadata Analysis Sample - Summary
Importance: High

Classification: CONFIDENTIAL//SI

Refs: A. Meeting [redacted] - 29 April 2014
B. [redacted]

Morning everyone,

First thanks for taking the time yesterday to help prepare us for the session later today. It was most appreciated.

As promised yesterday I have been able to piece together (most of) the answer to the question about the metadata sample that the IP Profiling analysis was conducted against.

A) Metadata type and period

The metadata consisting of international [redacted] generated by either a [redacted] was copied from the [redacted] It was a two-week metadata sample consisting of [redacted] events from [redacted]

B) System interaction

[redacted] At no time was any of this metadata shared with anyone either within CSE or external to CSE (i.e. 2nd parties) from this location in any form [redacted] As you saw yesterday the output is completely minimized and at no time contains any user attributable information, nor can it be reverse-engineered to reveal it.

C) Current status

[redacted] and I will share this information with you once I get it.

If you have any questions please don't hesitate to contact me.

Hope this helps. Cheers.

[redacted]

CSE/CST
SLT/[redacted]
[redacted]

s.15(1) - DEF

[redacted]

From: Bruce, Shelly D
Sent: February-03-14 11:08 AM
To: [redacted]
Subject: FW: Deck notes

Classification: TOP SECRET//SI//Canadian Eyes Only

FYI.

From: [redacted]
Sent: February-03-14 8:32 AM
To: [redacted]
Cc: Rochon, Dominic J; McLaughlin, Andrew J (Andy); [redacted] Ommanney, John L; [redacted]
Subject: Deck notes

Classification: TOP SECRET//SI//Canadian Eyes Only

Here are some notes on the deck. Let me know if you want more detail.

Red is TS//SI and will reveal things we don't want (or wouldn't have wanted) people to know.

Overall, presentation is about a number of different activities:

- The importance (and challenge) of accurate IP geolocation
- Ways to profile IPs so that we can quickly characterize similar IPs in the foreign target space
- Operational scenarios that require new ways to identify IPs in time and space when targets are trying to evade us

These are advanced analytics that would reveal the sophistication of CSE's SIGINT capabilities, methods and techniques against a backdrop of a very complicated internet-based operating environment and [redacted] To delve deeper into the underlying analysis would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.

Slide 1 (title slide) identifies that this is work was done by a tradecraft developer (aka data scientist, and not a target analyst) who works in the network analysis centre (whose focus is characterizing networks)

Slide2 sets the scene by noting that we cannot rely on commercial databases when IP geolocation is critical

- for example, a commercially registered IP in Canada would be found in the middle of nowhere—we KNOW this is untrue
- we want to use the info at our disposal to improve the accuracy of commercial reference data because we
    - WANT to know where our foreign targets are for <u>obvious operational reasons</u>, and

s.15(1) - DEF

s.15(1) - IA

- NEED to know where our foreign targets are for important compliance reasons.

Slide 3 lays out the purpose of the multi-part presentation: These are advanced analytics that would reveal the sophistication of CSE's SIGINT capabilities against a backdrop of a very complicated internet-based operating environment.

- How can we develop richer context around IPs to raise our confidence in what we are seeing? e.g. if it looks like this pattern of dots, it is probably an internet café
- Can we use this new knowledge to tip (or alert) us to when our targets interact in this space? [redacted]
- Can we use this new knowledge to find our targets, even when they are trying to evade our detection? [redacted]

Slides 4 – 8 describe the approach taken by the network analyst to characterize a travel node, in this case an airport

- Uses snapshot of historical, i.e. already collected metadata—no new effort launched
- Wants to establish patterns of activity around the IP during that snapshot to better characterize it—so that we can find similar patterns again elsewhere
- Tools used—commercial data (Quova, now called Neustar), [redacted]
- Source of metadata—[redacted]
- **To delve any deeper into the underlying analysis would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slides 9 show the results of the analysis of this first exercise to model activity around a travel node.

- Dots represent network activity and identify the global distribution of IPs associated with the other foreign airports from a network perspective
- **To delve any deeper into the underlying analysis would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 10 shows the same data as previous slide but notes the importance of accurate geolocation as a starting point, otherwise all subsequent analysis is erroneous, i.e. if your airport is the IP located by commercial data sources to be in the middle of a lake, then the rest of your data is probably wrong.

Slides 11 – 18 use the same approach to characterize related IPs to see if similar network activity patterns can be developed

- **To delve any deeper into the underlying analysis would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 19 - 20 summarize the findings and show the potential operational application of this exercise in a global context. [redacted]

- **To delve any deeper into the operational capacity to apply these models would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

s.15(1) - DEF

s.13(1)(a)

<<IMPORTANT INFO: End of this model, and end of this sample of historical metadata>>

Slide 21 outlines a new problem where targets use multiple devices (e.g. phones or other) to communicate with different parties, making it difficult to put the entire picture of activity together

- **Here we have just alerted our targets to the fact we know they use this technique and that we have developed or are developing methods to defeat their deception**

Slides 22 - 23 outline an approach to testing a hypothesis to discover this target behaviour

- The "sweep" of 300K IDs was done from a historical sample of metadata extracted from CSE's foreign intelligence collection, i.e. intercept from targets that are positively identified as foreign and outside Canada, and which correspond to GC priorities
- New analytics were successfully applied to filter through the 300K possibilities and identify 19 leads that would require follow on analysis, for example, the model that was produced in the earlier part of the presentation to help us understand if the target was at an internet café or other public access point
- **To delve any deeper into the operational capacity to apply these models would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 24 is the result of the metadata analysis

- **To delve any deeper into the operational capacity to apply these models would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 25 reveals the type of computing power that is required to conduct these analytics in operational scenarios.

- CARE is [redacted] (CSE [redacted] hence the reference)
- The work described in the presentation, however, was not done jointly with NSA, as reported by the media
- **As a rule, CSE would not expose the technology we use as that allows those we are targeting insight into our capabilities. To delve any deeper into the operational capacity to apply these models would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 26 indicates that we were successful in identifying new tradecraft that could be applied in operational scenarios involving foreign targets and indicates we are enhancing [redacted] **To delve any deeper into the operational capacity to apply these models would risk exposing specific capabilities, methods and techniques which, under SOIA, we are prohibited from doing.**

Slide 27 [redacted] slide was redacted entirely

Shelly Bruce | *SIGINT Deputy Chief/Chef adjoint SIGINT*
Communications Security Establishment/Centre de la sécurité des télécommunications
| *SLT* [redacted] | *613.991.7140;* [redacted]

s.15(1) - DEF

[redacted]

From:	Bruce, Shelly D
Sent:	February-03-14 12:59 PM
To:	[redacted]
Subject:	FW: Additional Qs and As

Classification: UNCLASSIFIED//CSE OFFICIAL USE ONLY

From: [redacted]
Sent: February-03-14 8:48 AM
To: Bruce, Shelly D
Subject: FW: Additional Qs and As

Classification: UNCLASSIFIED//CSE OFFICIAL USE ONLY

The latest Q&A

[redacted]

From: Ommanney, John L
Sent: February-03-14 8:45 AM
To: [redacted]
Subject: FW: Additional Qs and As

Classification: UNCLASSIFIED//CSE OFFICIAL USE ONLY

Here are the latest.

From: [redacted]
Sent: February-02-14 5:11 PM
To: Ommanney, John L
Cc: Nolan, Corinne M; Rochon, Dominic J
Subject: Additional Qs and As

Classification: UNCLASSIFIED//CSE OFFICIAL USE ONLY

Bringing up copies. E-copy for use if required.

s.15(1) - DEF

Potential Qs and As Released D...

[redacted]
Strategic Policy | Politiques stratégiques
EDB [redacted]
[redacted]

Q.1 If your business is foreign intelligence, why would you collect Canadian metadata or look at travellers in Canada?

- Metadata is technical information used to route communications, and not the contents of a communication.
- CSEC cannot and does not single out Canadian metadata for collection. The internet is large and complex, involving 3.5 billion users and 1800 petabytes of information that travel the globe each day, ignoring geographic and national boundaries. This complexity of global communications networks means that Canadian communications are comingled with international communications. In this context it is impossible for CSEC to collect exclusively foreign metadata.
- Metadata is required to ensure our activities are directed at foreign targets outside of Canada. For example, we must be able to use metadata to know when one of our foreign targets may be entering Canada. In which case, we must cease any intelligence coverage and, through intelligence reporting, advice the RCMP and CSIS so they can conduct any further follow-up.
- More importantly, metadata is essential to fulfill our mandate to collect foreign intelligence. CSEC uses metadata analysis techniques, such as those described in the presentation, to develop an understanding of the global networks used by our foreign intelligence targets.
- Foreign terrorist targets actively seek to hide in plain sight, to disguise their communications in the bustle and noise of urban life in order to evade detection
- It is essential for any foreign intelligence agency to be able to better understand the types of networks foreign targets use and how their behaviours might appear on those networks.
- For this reason, metadata is also used to build models to understand how networks operate in order to locate our legitimate foreign intelligence targets outside Canada.
- Without moving into operational specifics, I can state that the model illustrated in the presentation has been used in CSEC's efforts to gather foreign intelligence related to foreign terrorist targets. Within the last 12 month period, I am aware of at least 2 cases where this model has been used to identify foreign terrorist threats affecting Canadian and allied interests.

Q.2 How can you say that Canadians were not tracked?

- If CSEC were to track anyone, as we do with legitimate foreign targets outside Canada:
  - We would need to know who they are;
  - We would need to actively locate and find the individual; and
  - We would need to monitor their movements in real time.

- That was not the purpose or the result of this exercise.
- The goal was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport, so that CSEC could then apply this model for the purpose of gathering foreign intelligence.
- This work involved a snapshot of historical metadata collected from the global internet.
- We did not use this data to identify any individual Canadian or person in Canada.
- The data was only used to paint a picture of the pattern of network use in certain types of facilities with public internet access. This is what you see in the presentation, patterns of dots.

Q.3 How can you say that this activity was legal when the law says you cannot direct your activities at Canadians or persons in Canada?

- CSEC is authorized to acquire information in order to provide foreign intelligence under the *National Defence Act*.
- To fulfill this mandate, CSEC is authorized to collect and analyze metadata from the global information infrastructure.
- We use metadata to understand global communications networks so that we can find our targets in a vast sea of communications, and direct our activities at these legitimate foreign intelligence targets outside Canada in order to better understand their capabilities and intentions.
- These communications networks are complex, vast, borderless and rapidly changing, and foreign and Canadian communications are intermingled.
- As a result, CSEC collects and analyses metadata, so that we can better understand these networks, and so that we can ensure we are only directing our foreign intelligence activities at foreign targets outside of Canada
- That's what this exercise was: analyzing a snapshot of historical metadata from the global internet to build an analytical model of typical network activity patterns around a public access point – like an airport.
- The purpose of the model was solely to better understand what these patterns look like so that we can more effectively and quickly direct our foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers.
- This use of metadata is authorized under the *National Defence Act* and subject to conditions established under a Ministerial Directive. We recognize that metadata may contain information that has a privacy interest and we take strict measures to protect the privacy of Canadians and persons in Canada.

Q.4 How can you assure Canadians that their privacy was not violated through this activity?

- CSEC did not collect the content of any private communications.
- In this case, metadata, which does not include the content of a communication, was analysed for the sole purpose of developing an analytical model of patterns of network communication. This model was developed for application in identifying foreign threats.
- We did not use this data to identify any individual Canadian or person in Canada.
- All of CSEC's activities, including analytic activities involving the use of metadata in this exercise, include measures that protect the privacy of Canadians as well as the privacy of persons in Canada. These include conditions imposed by a Ministerial Directive, and which have been clearly articulated in CSEC policy.
- The independent CSE Commissioner has reviewed out metadata activities multiple times. He has never found CSEC to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.
- We recognize and acknowledge that many of our activities have privacy implications and we take this seriously. For that reason within CSEC there are multiple structures in place to ensure the privacy of Canadians is strictly protected. These include:
    - Active **monitoring of internal processes** and an internal audit and evaluation function;
    - A dedicated group of CSEC personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
    - **Executive control and oversight;**
    - An on-site **legal team** of 8 lawyers from the Department of Justice that works closely to provide independent legal advice to CSEC staff; and
    - **External review** by the CSE Commissioner as well as the Privacy Commissioner.

If pressed on how the personal information was protected

- While metadata is largely used to manage and route communications, we recognise that metadata may contain information that has a privacy interest.
- Under the *National Defence Act* and consistent with our other legal obligations CSEC must take steps to protect the privacy of Canadians and persons in Canada in its use and retention of information. This includes not only private communications but other information that has a privacy interest

- We do this through concrete steps such as implementing strict controls on the use, retention, sharing and access to this information.
- The multiple structures we have in place for process monitoring, policy compliance, executive control, legal advice and external review ensure that these measures to protect privacy are followed.
- The CSE Commissioner reviews our measures to protect privacy in every single review he undertakes.

Q.5 Who approved this operation?

- Let me clarify that this was not an operation.
- This was an exercise using a snapshot of historical metadata to build a mathematical, analytical model. It was not subject to ministerial approval.
- CSEC's use of metadata is authorized under the *National Defence Act* and is subject to conditions set out in a Ministerial Directive that was signed in 2011.
- The independent CSE Commissioner regularly reviews CSEC activities, including our activities involving metadata.

Q.6 I hear that CSEC conducted this activity as a trial run for the NSA and other international partners?

- CSEC conducts its foreign intelligence activities in accordance with intelligence priorities set by the Government of Canada.
- CSEC did not conduct this activity on behalf of the NSA or any other partner agency. This was a CSEC effort to develop a mathematical analytic model that can refine CSEC's understanding of communication networks and identify foreign targets.
- While we work closely with our allies to address threats that affect our common interests, no foreign partner can ask another to do something it cannot legally do itself.
- CSEC does not take direction from any outside organization. We are accountable to the Minister of National Defence, the Government of Canada and Parliament.

Q.7 Is this "trial run" now a fully operational program?

- Contrary to media speculation, the subject of this slide presentation is an analytical model. It does not represent an operational program not is it directed at Canadians. It only illustrates a validation exercise of an analytic technique for application in directing our lawful activities at foreign entities outside Canada, such as foreign terrorist targets.

Q.8 How did you obtain this data about travellers at the airport? Who or what is your "special source"?

- No data was collected through any monitoring of the operations of any airport.
- To provide more specific details than those already released by the press would reveal highly classified techniques and capabilities. Since this could cause further injury to Canada's national security, I am not permitted under the law to disclose any further details.

If pressed on any particular slide detail

- I would be happy to discuss and clarify for the committee the overall nature of the exercise and the analytical model described in the document.
- However, I cannot provide any more specific details that could cause further injury to Canada's national security. That would be contrary to the law.
- While the document has been published, it has been released without proper authorization and still contains highly classified details about techniques and capabilities.

s.15(1) - DEF

[redacted]

From: [redacted]
Sent: February-03-14 12:57 PM
To: [redacted]
Cc:
Subject: RE: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

I had this [redacted]. and again, no one has raised any compliance/lawfulness questions...
Many of these concepts are hard to explain in layman's term, so that's why there is extra attention on the choice of words used (i.e to make sure we don't mislead and to make sure if we don't limit the scope of any future activities)

[redacted]

From: [redacted]
Sent: February-03-14 12:51 PM
To: [redacted]
Cc:
Subject: FW: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

Sir,

FYI, the initial activity/feedback from [redacted]

Cheers.

[redacted]

From: [redacted]
Sent: October-16-12 7:20 PM
To: ([redacted]
Subject: RE: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

Hello,

I believe I used this string last week to request that we put an end to email exchanges on this issue, since there were many on the go (though I failed to locate me message to that effect...)

s.15(1) - DEF

There's been time to examine this network analysis project in the meantime and obtain more details on the nature of this research using [redacted]metadata.

The overall thrust of the research aims to provide greater resolution of IP addresses through the identification and analysis of patterns of IPs that emerge in a number of different use settings.

The value of enhancing the resolution of these IPs is that it ultimately allows for a greater understanding of the technical details, characteristics and specifications of communications networks and an enhanced ability to determine the locations of communications in specific circumstances.

[redacted] will work with the [redacted] to ensure that the project's objectives are adequately captured and clearly reflect their focus, so that there is no potential ambiguity about the nature of this work, which lies squarely in the realm of acceptable network analysis activities.

Thanks everyone for the chance to discuss this issue and for taking the time to engage.

[redacted]

~~~~~~~~~~~

[redacted]

CSEC-CSTC | SLT [redacted]

[redacted]

From: [redacted]
Sent: October-09-12 12:21 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

[redacted]

s.21(1)(b)

[redacted]

[redacted]

CSE Canada/CST Canada
~~~~~~~~~~~

s.15(1) - DEF

SLT/[redacted]
Secure: [redacted]
Non-Secure: [redacted]

From: [redacted]
Sent: October-09-12 11:13 AM
To: [redacted]
Cc:
Subject: RE: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

s.21(1)(b)

HI [redacted]

[redacted] We will examine it further and get back to you [redacted]

[redacted]

[redacted]
green/vert [redacted] **black/noir** [redacted]
SLT/[redacted] and SLT/[redacted]
CSE/CST Ottawa

From: [redacted]
Sent: October-09-12 11:03 AM
To: [redacted]
Cc: [redacted]
Subject: FW: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI//Canadian Eyes Only

s.21(1)(b)

Good morning,

Please see attached presentation [redacted]

s.15(1) - DEF

cheers

[redacted]
Manager, [redacted]

From: [redacted]
Sent: September-27-12 4:38 PM
To: [redacted]
Subject: [redacted] IP Profiling Analytics

Classification: TOP SECRET//SI

<< File: IP Profiling Analytics.pptx >>

[redacted]

From: [redacted]
Sent: April-10-14 10:38 AM
To: [redacted]
Cc: [redacted]
Subject: OCSEC Metadata Review - Follow-on questions IP Profiling

Importance: High

Classification: SECRET//SI

[redacted]

I have been given a heads up from [redacted] based on an email request from the OCSEC Legal Advisor that they would like to gain a better understanding of SIGINT metadata analysis for numerous activities (e.g. IP Profiling, [redacted] [redacted]

As such they will be requesting a meeting, coordinated by [redacted] as described here:

"In order to have a better understanding of SIGINT metadata analysis activities, we would appreciate it if you could set up the following briefings and demonstrations:

1- We would like to meet [redacted] again in order to ask him some follow-up questions to the briefing he already provided us. We would also appreciate seeing a demonstration of how he undertook the IP profiling analytics.

…"

They are going to provide a set of questions for the presenters which I will share with you as soon as I get it. We can discuss once [redacted] returns on how best to present the demonstration/information to meet their request.

Cheers.

[redacted]

CSE/CST
SLT/[redacted]
Secure: [redacted]
Non-Secure: [redacted]

s.15(1) - DEF

s.20(1)(a)
s.20(1)(b)
s.20(1)(c)
s.20(1)(d)

[redacted]

From: [redacted]
Sent: January-29-14 7:05 AM
To: Bruce, Shelly D
Cc: [redacted]
Subject: IP Profiling - History of Analytic/CARE

Importance: High

Classification: CONFIDENTIAL//SI

Morning Ma'am,

H/W the best estimate of what [redacted] has put together for the data that was used to develop the analytics as well as some information about the tradecraft environment system, Collaborative Analysis Research Environment (CARE).

The [redacted] first learned about CARE in late [redacted] at the [redacted] as it came up in some slides from [redacted] Group. CARE is a big-data high performance data science platform for developing world-class analytics. The CARE platform is by an [redacted] It builds on the platform [redacted] At CSE the project is managed by the Joint Research Office with whom we work closely. [redacted] is the lead CARE developer at CSE and provides vital feedback on issues, requested enhancements etc. to [redacted], the JRO lead, who then passes it on to [redacted]

[redacted] analytical results which appeared in the presentation were based on two-week random metadata pulls from [redacted] using metadata that was collected [redacted] At that time we didn't have the CARE platform so the network analysis profiling [redacted] was being done with our [redacted] We would get a [redacted]

Throughout the next year [redacted] would continue to work with the metadata in this way (i.e. getting a two-week random sample of metadata events so as to continue to refine the tradecraft and build a reference base to compare one set of data versus another. All data would have been from [redacted] Once we had the CARE environment setup in [redacted] we would then get the same type of metadata events but from that time period.

So effectively, CARE was introduced into CSE sometime in [redacted] and we began using it in earnest once we learned about it and were given accounts and were able to get copies of the metadata events to work with. This is how we were able to compare the speed differences in the platforms for creating the tradecraft and getting the results.

[redacted]

Hope this helps. Cheers.

[redacted]

CSE Canada/CST Canada

s.15(1) - DEF

SLT/[redacted]
Secure [redacted]
Non-Secure: [redacted]

s.15(1) - DEF

[redacted]

From: [redacted]
Sent: January-28-14 4:18 PM
To: Bruce, Shelly D; [redacted]
Subject: NS review of IP profiling

Classification: TOP SECRET//SI//Canadian Eyes Only

Overall, presentation is about Analytics to profile IP addresses/ranges in order to characterise them in an effort to refine the SIGINT development effort in pursuing targets in a complex communication environment. These are advanced analytics that would showcase the sophistication of CSE's SIGINT capabilities.

- Slide 1: Title: identification of an [redacted] group – might spur "journalistic" sources to seek additional information about the group
  - IoD
    - Reveals name of a CSE employee and his [redacted]
- Slide 2: nature of IP profiling and challenges with accuracy of the data.
  - IoD:
    - Reveals the use of a CDN IP derived from a commercial database to demonstrate the challenges with the accuracy of IP Geolocation
    - Reveals the original owner of the IP ([redacted]
- Slide 3: Objective of the effort, setting the stage for the problem set and the rest of the presentation
- Slide 4: the seed of this effort is around travellers and using Wi-Fi hotspot at an intl. airport as a starting point
  - IoD:
    - [redacted]
    - reveals SIGINT techniques and methodologies
- Slide 5: scope of profiling travel nodes
  - IoD
    - reveals SIGINT techniques and methodologies
- Slide 6: IP profiling over time around travel nodes
  - IoD
    - reveals SIGINT techniques and methodologies
- Slide 7: theory vs what real data reveals
  - IoD:
    - [redacted]
    -
    - Reveals SIGINT sources, methods and capabilities
- Slide 8: overview of the data used in the development of this analytic
  - IoD:
    - [redacted]

    - [redacted]
    - reference to having seed knowledge of a Canadian Airport Wi-Fi IP address
- Slide 9: geo plot of IP activities starting from a CDN airport intl. terminal as a seed
  - IoD
    - Reveals the use of a IP of CDN airport as a seed ; while this analysis is based purely on metadata (no content was ever collected), this would be damaging in putting into question CSE SIGINT's use of CDN metadata
    - Reveals SIGINT's capabilities in profiling geo-hops to track roamers
- Slide 10: slide depicting the impact of a "what-if" scenario around the erroneous geolocation of the initial seed IP
  - IoD
    - Similar to slide 9 but in the context of erroneous geolocation based on commercial datasets
- Slide 11: demonstrated the ability to characterise at a high level the previous and next hops centered around the CDN airport intl terminal
  - IoD
    - SIGINT tradecrafts and techniques
- Slide 12: based on data collected, the profile of another CDN airport is noted
  - IoD
    - While similar to the methodology used in slide 9, this slide perpetuates the issue associated with the use of CDN metadata
    - SIGINT methods
- Slide 13-17: each slide demonstrate the profile of a unique entity based on the pattern of user ID seen over time
  - IoD
    - SIGINT's advanced analytics being able to characterize an entity based (purely on metadata) on the pattern of user ID seen
    - Building on slide 7 and slide 9 (the use of a sample from CDN special source to characterize a CDN intl. airport), the examples outlined in the 5 slides imply that part of this effort was to characterise a Hotel, an enterprise, a coffee shop, a library, a wireless gateway based on CDN metadata
    - SIGINT methods and techniques
- Slide 18: slide specific to the characterization of a wireless gateway
  - IoD
    - SIGINT methods and techniques
- Slide 19: why IP profiling is important to SIGINT
  - IOD: disclosure of the applicability of this analytic to real SIGINT missions
    - [redacted]
    - SIGINT methods and techniques
- Slide 20: summary of the analytical hypothesis presented in the 19 previous slides
  - IOD:
    - Use of "sweep" can imply the ability to [redacted] (metadata)
    - SIGINT methods and techniques

s.15(1) - DEF

- Slides 21-25 demonstrate the use of the IP analytic tradecrafts in support of the SIGINT's efforts to tackle the challenges associated with a kidnaping case (who is behind a ransom call, where are they, can we track them and work our way back to where the hostage is being held)
  - IOD
    - damaging in disclosing what SIGINT would be looking for to associate and correlate timing and geolocation information associated with ransom calls
- Slide 21: Hostage problem statement
- Slide 22: Solution outline
  - IOD
    - High level outline of the recipe used to tackle this problem
- Slide 23: Proof of concept using a sample of SIGINT data
  - IOD
    - Questions could be raised as to the nature of the sample (is it Canadian ? metadata etc...)
- Slide 24: results of using the analytic on test data and how the presence of the kidnapper/target would be detected
  - IoD
    - SIGINT methods and techniques
- Slide 25: challenges associated with large data sets and the advantages of using CARE
  - IoD
    - Reveals SIGINT sources, tradecrafts, capabilities and relationships
    - CARE is a product of [redacted]
- Slide 26: overall summary of the deck
  - IoD
    - Reveals the value of IP profiling
    - [redacted]
    - Advanced technique to contact chain across air-gaps
    - SIGINT methods, techniques, capabilities
- Slide 27: same as slide 1

[redacted]

[redacted]

CSEC's Use of Metadata
Senate Committee on National Security and Defence
February 4, 2014

CSE's role is to collect information on foreign targets from the global information infrastructure – the Internet. To do this, we need to understand how millions of communications networks function, how they are constantly changing and how foreign targets make use of them.

The document refers to a model we were trying to build of the typical communications patterns around public internet access points – in this case an airport. This work relied on metadata. Metadata is data about a communication, but not the contents of a communication itself. It is used by computers to manage or route communications over global networks. It does not include any content of emails, phone messages, text messages, photos.

CSE collects metadata from the global internet in order to:

1. Understand constantly changing global communications networks to know how to find our target in a sea of billions of communications
2. We use it to ensure our intelligence collection is directed at foreign targets outside of Canada and to avoid targeting Canadians' communications.

This exercise involved using a snapshot of historical metadata collected from the global internet. No data was collected through any monitoring of the operations at any airport.

This was not and is not an operational surveillance program. That was not the purpose or the result of this exercise. We weren't targeting or trying to find anyone or monitor any individuals' movements in real time.

The purpose was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport – which is what you see in the document, patterns of dots.

The goal was to build a mathematical, analytical model. The end result of this work was formulas, algorithms, software.

The reason we did this was to develop a model that could help us find legitimate foreign targets – terrorists, hostage takers, foreign intelligence agents. For example, we may have hostages taken in a foreign city – possibly Canadians or citizens of one of our allies. Our challenge is - how do we find our foreign targets in a sea of billions and billions of communications?

This analytical model can help us in two ways:

First - It helps us to narrow our search in a foreign remote region or large city – filtering from millions of possibilities to a few.

Second - we know terrorists or hostage takers will often use public places to access the internet because they are trying to hide in plain sight. This model helps us to identify where that contact may be coming from – a café, a hotel, an airport.

This model can save time and work during an incident where time is critical. It increases our chance of success. I am aware of at least 2 cases in the past year where this model has been and is being used to help identify foreign terrorist threats.

The collection and use of metadata to analyze global networks is authorized under the *National Defence Act*. This work was conducted under conditions set out in a Ministerial Directive on metadata signed in 2011.

No Canadians' private communications were targeted, collected or used. We did not use this data to identify any individual Canadian or person in Canada. As with all of our activities, measures were in place and applied to protect the privacy of Canadians.

Our collection and use of metadata, including for network analysis, has been reviewed by successive Commissioners 5 times since 2003, most recently in 2011, and found to be lawful. The Commissioner approved a review in 2012 which is underway.

Q.1 If your business is foreign intelligence, why would you collect Canadian metadata or look at travellers in Canada?

- Metadata is technical information used to route communications, and not the contents of a communication.
- CSEC cannot and does not single out Canadian metadata for collection. The internet is large and complex, involving 3.5 billion users and 1800 petabytes of information that travel the globe each day, ignoring geographic and national boundaries. This complexity of global communications networks means that Canadian communications are comingled with international communications. In this context it is impossible for CSEC to collect exclusively foreign metadata.
- Metadata is required to ensure our activities are directed at foreign targets outside of Canada. For example, we must be able to use metadata to know when one of our foreign targets may be entering Canada. In which case, we must cease any intelligence coverage and, through intelligence reporting, advice the RCMP and CSIS so they can conduct any further follow-up.
- More importantly, metadata is essential to fulfill our mandate to collect foreign intelligence. CSEC uses metadata analysis techniques, such as those described in the presentation, to develop an understanding of the global networks used by our foreign intelligence targets.
- Foreign terrorist targets actively seek to hide in plain sight, to disguise their communications in the bustle and noise of urban life in order to evade detection
- It is essential for any foreign intelligence agency to be able to better understand the types of networks foreign targets use and how their behaviours might appear on those networks.
- For this reason, metadata is also used to build models to understand how networks operate in order to locate our legitimate foreign intelligence targets outside Canada.
- Without moving into operational specifics, I can state that the model illustrated in the presentation has been used in CSEC's efforts to gather foreign intelligence related to foreign terrorist targets. Within the last 12 month period, I am aware of at least 2 cases where this model has been used to identify foreign terrorist threats affecting Canadian and allied interests.

Q.2 How can you say that Canadians were not tracked?

- If CSEC were to track anyone, as we do with legitimate foreign targets outside Canada:
  - We would need to know who they are;
  - We would need to actively locate and find the individual; and
  - We would need to monitor their movements in real time.

- That was not the purpose or the result of this exercise.
- The goal was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport, so that CSEC could then apply this model for the purpose of gathering foreign intelligence.
- This work involved a snapshot of historical metadata collected from the global internet.
- We did not use this data to identify any individual Canadian or person in Canada.
- The data was only used to paint a picture of the pattern of network use in certain types of facilities with public internet access. This is what you see in the presentation, patterns of dots.

Q.3 How can you say that this activity was legal when the law says you cannot direct your activities at Canadians or persons in Canada?

- CSEC is authorized to acquire information in order to provide foreign intelligence under the *National Defence Act*.
- To fulfill this mandate, CSEC is authorized to collect and analyze metadata from the global information infrastructure.
- We use metadata to understand global communications networks so that we can find our targets in a vast sea of communications. Global communications networks are complex, vast, borderless and rapidly changing, and foreign and Canadian communications are intermingled.
- CSEC collects and analyses metadata, so that we can better understand these networks, and so that we can ensure we are only directing our foreign intelligence activities at foreign targets outside of Canada.
- Foreign intelligence reveals the motivations, intentions and capabilities of our foreign targets. To find our foreign targets, we first need to understand the global network, how it operates, and then how our targets operate on that global network.
- That's what this exercise was about: analyzing a snapshot of historical metadata from the global internet to build an analytical model of typical network activity patterns around a public access point – like an airport.
- We did not use this data to identify any individual Canadian or person in Canada.
- The sole purpose of the model was to better understand what these patterns look like so that we can more effectively and quickly direct our foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers.
- This use of metadata is authorized under the *National Defence Act* and subject to conditions established under a Ministerial Directive. We recognize that metadata may contain information that has a privacy interest and we take strict measures to protect the privacy of Canadians and persons in Canada.

Q.4 How can you assure Canadians that their privacy was not violated through this activity?

- CSEC did not collect the content of any private communications.
- In this case, metadata, which does not include the content of a communication, was analysed for the sole purpose of developing an analytical model of patterns of network communication. This model was developed for application in identifying foreign threats.
- We did not use this data to identify any individual Canadian or person in Canada.
- All of CSEC's activities, including analytic activities involving the use of metadata in this exercise, include measures that protect the privacy of Canadians as well as the privacy of persons in Canada. These include conditions imposed by a Ministerial Directive, and which have been clearly articulated in CSEC policy.
- The independent CSE Commissioner has reviewed out metadata activities multiple times. He has never found CSEC to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.
- We recognize and acknowledge that many of our activities have privacy implications and we take this seriously. For that reason within CSEC there are multiple structures in place to ensure the privacy of Canadians is strictly protected. These include:
    - Active **monitoring of internal processes** and an internal audit and evaluation function;
    - A dedicated group of CSEC personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
    - **Executive control and oversight;**
    - An on-site **legal team** of 8 lawyers from the Department of Justice that works closely to provide independent legal advice to CSEC staff; and
    - **External review** by the CSE Commissioner as well as the Privacy Commissioner.

If pressed on how the personal information was protected

- While metadata is largely used to manage and route communications, we recognise that metadata may contain information that has a privacy interest.
- Under the *National Defence Act* and consistent with our other legal obligations CSEC must take steps to protect the privacy of Canadians and persons in Canada in its use and retention of information. This includes not only private communications but other information that has a privacy interest

- We do this through concrete steps such as implementing strict controls on the use, retention, sharing and access to this information.
- The multiple structures we have in place for process monitoring, policy compliance, executive control, legal advice and external review ensure that these measures to protect privacy are followed.
- The CSE Commissioner reviews our measures to protect privacy in every single review he undertakes.

Q.5 Who approved this operation?

- Let me clarify that this was not an operation.
- This was an exercise using a snapshot of historical metadata to build a mathematical, analytical model. It was not subject to ministerial approval.
- CSEC's use of metadata is authorized under the *National Defence Act* and is subject to conditions set out in a Ministerial Directive that was signed in 2011.
- The independent CSE Commissioner regularly reviews CSEC activities, including our activities involving metadata.

Q.6 I hear that CSEC conducted this activity as a trial run for the NSA and other international partners?

- CSEC conducts its foreign intelligence activities in accordance with intelligence priorities set by the Government of Canada.
- CSEC did not conduct this activity on behalf of the NSA or any other partner agency. This was a CSEC effort to develop a mathematical analytic model that can refine CSEC's understanding of communication networks and identify foreign targets.
- While we work closely with our allies to address threats that affect our common interests, no foreign partner can ask another to do something it cannot legally do itself.
- CSEC does not take direction from any outside organization. We are accountable to the Minister of National Defence, the Government of Canada and Parliament.

Q.7 Is this "trial run" now a fully operational program?

- Contrary to media speculation, the subject of this slide presentation is an analytical model. It does not represent an operational program not is it directed at Canadians. It only illustrates a validation exercise of an analytic technique for application in directing our lawful activities at foreign entities outside Canada, such as foreign terrorist targets.

Q.8 How did you obtain this data about travellers at the airport? Who or what is your "special source"?

- No data was collected through any monitoring of the operations of any airport.
- To provide more specific details than those already released by the press would reveal highly classified techniques and capabilities. Since this could cause further injury to Canada's national security, I am not permitted under the law to disclose any further details.

If pressed on any particular slide detail

- I would be happy to discuss and clarify for the committee the overall nature of the exercise and the analytical model described in the document.
- However, I cannot provide any more specific details that could cause further injury to Canada's national security. That would be contrary to the law.
- While the document has been published, it has been released without proper authorization and still contains highly classified details about techniques and capabilities.

Questions and Answers for the Chief: Unauthorized Disclosure on Airport Metadata Analysis

Q.1 What were you doing in the project described in this document?

- The document refers to a model we were trying to build of the typical communications patterns around public internet access points – in this case an airport. This is what you see in the document: patterns of dots.
- This work relied on metadata. Metadata is data about a communication, not the contents of a communication itself. It is technical information used by computers to manage or route communications over global networks. It does not include any content of the communications – no emails, no phone messages, no text messages, no photos, no content.
- CSE collects metadata from the global internet in order to:
    - Understand the constantly changing global communications networks to know how to find legitimate foreign targets in a sea of billions of bits of communications.
    - Ensure our intelligence collection is directed at foreign targets outside of Canada.
- The purpose of the exercise was to develop a model to help us find legitimate foreign targets – terrorists, hostage takers, foreign intelligence agents. For example, we may have hostages taken in a foreign city – possibly Canadians or citizens of one of our allies. How do we find our foreign targets in a sea of billions and billions of communications?
- This exercise involved using a snapshot of historical metadata collected from the global internet. No data was collected through any monitoring of the operations at any airport. This was not and is not an operational surveillance program.
- No Canadians' private communications were targeted, collected or used. We did not use this data to identify any individual Canadian or person in Canada. As with all of our activities, measures were in place and applied to protect the privacy of Canadians.
- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada.

SHORT FORM RESPONSE THEREAFTER

- As I have already outlined in detail in my recent appearance before Senate committee, the activity described in the document was an exercise to develop a mathematical model for the sole purpose of finding legitimate foreign targets under our legal mandate for foreign intelligence. No data was collected from monitoring the operations at any Canadian airport and no private communications were collected. The independent CSE Commissioner has looked into this matter and publicly confirmed that this analysis did not involve any 'mass surveillance', that no Canadians or persons in Canada were tracked, and that no activity was directed at Canadians or persons in Canada.

Q.2 How was the data that was collected used?

- The data was used to build an analytical model of typical patterns of network activity around a public internet access point.
- This analytical model can help us fulfill our mandate in two ways:
  - o It helps us to narrow our search in a foreign remote region or large city – filtering from millions of possibilities to a few.
  - o Terrorists or hostage takers will often use public places to access the internet because they are trying to hide in plain sight. This model, which helped to identify typical patterns, helps us to identify where that contact may be coming from – a café, a hotel, an airport.
- Further, this model can save time and work during an incident where time is critical. It increases our chance of success. I am aware of at least 2 cases where this model has been used in the past year to help identify foreign terrorist threats.
- The collection and use of metadata to analyze and understand the global internet for the purpose of targeting foreign entities outside Canada is authorized under the *National Defence Act*.

Q.3 If your business is foreign intelligence, why would you collect Canadian metadata or look at travellers in Canada?

- Metadata is technical information used to route communications, and not the contents of a communication.

- CSE cannot and does not single out Canadian metadata for collection. The internet is large and complex, involving 3.5 billion users and 1800 petabytes of information that travel the globe each day, ignoring geographic and national boundaries. This complexity of global communications networks means that Canadian communications are comingled with international communications. In this context it is impossible for CSE to collect exclusively foreign metadata.

- Metadata is required to ensure our activities are directed at foreign targets outside of Canada. For example, we must be able to use metadata to know when one of our foreign targets may be entering Canada. In which case, we must cease any intelligence coverage and, through intelligence reporting, advise the RCMP and CSIS so they can conduct any further follow-up.
- More importantly, metadata is essential to fulfill our mandate to collect foreign intelligence. CSE uses metadata analysis techniques, such as those described in the document, to develop an understanding of the global networks used by our foreign intelligence targets.
- Foreign terrorist targets actively seek to hide in plain sight, to disguise their communications in the bustle and noise of urban life in order to evade detection
- It is essential for any foreign intelligence agency to be able to better understand the types of networks foreign targets use and how their behaviours might appear on those networks.
- For this reason, metadata is also used to build models to understand how networks operate in order to locate our legitimate foreign intelligence targets outside Canada.

Q.4 How can you say that this activity was legal when the law says you cannot direct your activities at Canadians or persons in Canada?

- CSE is authorized to acquire information from the global information infrastructure in order to provide foreign intelligence under the *National Defence Act*.
- To fulfill this mandate, CSE is authorized to collect and analyze metadata from the global information infrastructure.
- We use metadata to understand global communications networks so that we can find our targets in a vast sea of communications, and direct our activities at these legitimate foreign intelligence targets outside Canada in order to better understand their capabilities and intentions.
- Foreign and Canadian communications are intermingled on these communications networks which are complex, vast, borderless and rapidly changing.
- As a result, CSE collects and analyses metadata, so that we can better understand these networks, and so that we can ensure we are only directing our foreign intelligence activities at foreign targets outside of Canada
- That's what this exercise was: analyzing a snapshot of historical metadata from the global internet to build an analytical model of typical network activity patterns around a public access point – like an airport.
- We did not use this data to identify any individual Canadian or person in Canada.

- The sole purpose of the model was to better understand what these patterns look like so that we can more effectively and quickly direct our foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers.
- This use of metadata is authorized under the *National Defence Act.* Both the collection and use of metadata in this case was in accordance with the conditions set out in the current Ministerial Directive on metadata. The first Ministerial Directive, which accounted for this kind of network analysis, was signed in 2005. A new Ministerial Directive was submitted by my predecessor and signed by the Minister in 2011.
- Our collection and use of metadata, including network analysis, has specifically been reviewed by successive Commissioners six times since 2003, the most recent of which was submitted to the Minister in 2011, and were found to be lawful. The Commissioner has approved in 2012 a new review of metadata. Metadata is the kind of topic that the Commissioner regularly looks at and we are happy to cooperate with him in that review.
- The independent CSE Commissioner has also recently looked into this specific issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada.

Q.5 How can you assure Canadians that their privacy was not violated through this activity?

- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada,
- CSE did not collect the content of any private communications.
- In this case, metadata, which does not include the content of a communication, was analysed for the sole purpose of developing an analytical model of patterns of network communication. This model was developed for application in identifying foreign threats.
- We did not use this metadata to identify any individual Canadian or person in Canada.
- All of CSE's activities, including analytic activities involving the use of metadata in this exercise, include measures that protect the privacy of Canadians as well as the privacy of persons in Canada. These include conditions imposed by a Ministerial Directive, and which have been clearly articulated in CSE policy.
- The independent CSE Commissioner has reviewed our metadata activities multiple times, and as part of his current efforts, he is conducting another review of our use of metadata. He has never found CSE to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.

- We recognize and acknowledge that many of our activities, including the collection and use of metadata, have privacy implications and we take this seriously. For that reason within CSE there are multiple structures in place to ensure the privacy of Canadians is strictly protected. These include
  - Active **monitoring of internal processes** and an internal audit and evaluation function;
  - A dedicated group of CSE personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
  - **Executive control and oversight;**
  - An on-site **legal team** of 8 lawyers from the Department of Justice that works closely to provide independent legal advice to CSE staff; and
  - **External review** by the CSE Commissioner as well as the Privacy Commissioner.

Q.6 What kind of data did you collect and how was private information protected?

- While metadata is largely technical data used to manage and route communications, we recognise that metadata may contain information that has a privacy interest.
- Under the *National Defence Act* and consistent with our other legal obligations CSE must take steps to protect the privacy of Canadians and persons in Canada in its use and retention of information. This includes not only private communications but other information that has a privacy interest
- We do this through concrete steps such as implementing strict controls on the use, retention, sharing and access to this information.
- The multiple structures we have in place for process monitoring, policy compliance, executive control, legal advice and external review ensure that these measures to protect privacy are followed.
- The CSE Commissioner reviews our measures to protect privacy in every single review he undertakes.

Q.7 How can you say that Canadians were not tracked?

- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada.

- If CSE were to track anyone, as we do with legitimate foreign targets outside Canada:
    - We would need to know who they are;
    - We would need to actively locate and find the individual; and
    - We would need to monitor their movements in real time.
- That was not the purpose or the result of this exercise.
- The goal was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport, so that CSE could then apply this model for the purpose of gathering foreign intelligence.
- This work involved a snapshot of historical metadata collected from the global internet.
- We did not use this data to identify any individual Canadian or person in Canada.
- The data was only used to paint a picture of the pattern of network use in certain types of facilities with public internet access. This is what you see in the document, patterns of dots.

Q.8 Who approved this operation?

- Let me clarify that this was not an operation.
- This was an analytic exercise using a snapshot of historical metadata to build a mathematical, analytical model. It was not subject to ministerial approval.
- CSE's use of metadata is authorized under the *National Defence Act* and is subject to conditions set out in a Ministerial Directive that was signed in 2011..
- The independent CSE Commissioner regularly reviews CSE activities, including our activities involving metadata.

Q.9 Why did you develop this model in Canada? Why not an airport in another country?

- In order to fulfill our mandate to collect foreign signals intelligence in accordance with government intelligence priorities, we need to understand where our foreign targets are and how they communicate on global networks. In order to understand global networks we conduct network analysis and develop models, for which we require the use of metadata.
- This analysis took a snapshot from previously collected metadata and that was then used to test algorithms to describe patterns of public access behaviours on the Internet. This enables us to model how networks operate in order to locate our legitimate foreign intelligence targets, also outside Canada.
- The development of this model was done using a small subset of metadata that we had collected, as authorized under the law.

- In order to develop an accurate model we needed a thorough understanding of a network associated with a public internet access point. We used data where the parameters of the network could then be validated through publicly available and geographically accurate information.
- This way, when we use the model in a foreign country, where we know little about the conditions, we can be confident that the model is valid, robust and reliable, and will allow us to have high confidence in the accuracy of the resulting analysis.

Q.10 I hear that CSE conducted this activity as a trial run for the NSA and other international partners?

- CSE conducts its foreign intelligence activities in accordance with intelligence priorities set by the Government of Canada.
- CSE did not conduct this activity on behalf of the NSA or any other partner agency. This was a CSE effort to develop a mathematical analytic model that can refine CSE's understanding of communication networks and identify foreign targets.
- While we work closely with our allies to address threats that affect our common interests, no foreign partner can ask another to do something it cannot legally do itself.
- CSE does not take direction from any outside organization. We are accountable to the Minister of National Defence, the Government of Canada and Parliament.

Q.11 Is this "trial run" now a fully operational program?

- Contrary to media speculation, the subject of this slide presentation is an analytical model. It does not represent an operational program. It only illustrates a validation exercise of an analytic technique for application in directing our lawful activities at foreign entities outside Canada, such as foreign terrorist targets.
- The independent CSE Commissioner has also recently looked into this specific issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada.

Q.12 How did you obtain this data about travellers at the airport? Who or what is your "special source"?

- No data was collected through any monitoring of the operations of any airport.
- To provide more specific details than those already released by the press would reveal highly classified techniques and capabilities. Since this could cause further injury to Canada's national security, I am not permitted under the law to disclose any further details.

If pressed on any particular detail related to methods, capabilities, targets or operations:

- I would be happy to discuss and clarify for the committee the overall nature of the exercise and the analytical model described in the document.
- However, I cannot provide any more specific details that could cause further injury to Canada's national security. That would be contrary to the law.
- While the document has been published, it has been released without proper authorization and still contains highly classified details about techniques and capabilities.

TAB 34

UNAUTHORIZED DISCLOSURE: AIRPORT METADATA ANALYSIS

SPEAKING POINTS:

- CSE's work is vital to the security and safety of Canada and Canadians. By law, CSE only directs its foreign intelligence activities at foreign entities outside Canada.
- The Chief of CSE has appeared before Senate Committee to provide a full description of the analysis undertaken, which was for the sole purpose of finding legitimate foreign targets under CSE's legal mandate for foreign intelligence.
- The independent CSE Commissioner has reviewed CSE's metadata activities multiple times and has concluded they were lawful
- Further, the Commissioner has looked into this activity and publicly confirmed that this analysis did not involve any 'mass surveillance', that no Canadians or persons in Canada were tracked, and that no activity was directed at Canadians or persons in Canada.

FOR FURTHER INFORMATION:

- Chief, CSE

BACKGROUND INFORMATION

- The January 30, 2014 unauthorized disclosure of details from a highly classified CSE technical deck has led to allegations in the media and in Parliament that CSE is acting unlawfully by conducting mass surveillance and directing its foreign intelligence activities at Canadians.
- The classified document that was released is a technical presentation that outlines an exercise to build a mathematical model of typical network activity patterns around a public internet access point. The analysis conducted was based on a snapshot of historical metadata from the global internet.
- No data was collected from the monitoring of any airport. No private communications were targeted, collected or used. No data was used to identify any individual Canadian or person in Canada.

- The sole purpose of the model was to better understand what these network activity patterns look like so that CSE can more effectively and quickly direct its foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers who often seek to hide in plain sight by using public internet access points.
- The use of metadata to better understand global networks is essential to the fulfillment of CSE's foreign intelligence mandate.
- CSE acquires and analyses metadata pursuant to its mandate as set out in the *National Defence Act* and subject to all of the restrictions of the *Act*, including the restrictions on directing activities at Canadians or any person in Canada and the requirement to have measures in place to protect the privacy of Canadians. Any metadata-related activities are also subject to applicable ministerial directives, applicable ministerial authorizations, and various other policies and procedures put in place to provide comprehensive protection for the privacy of Canadians and persons in Canada.
- The CSE Commissioner has reviewed CSE metadata activities multiple times and has concluded they were lawful. The CSE Commissioner is currently conducting another review of CSE's metadata activities.
- Recently, the CSE Commissioner has posted an update to his website noting that he has looked into this specific activity and confirming that the analysis did not involve any 'mass surveillance', that no Canadians or persons in Canada were tracked, and that no activity was directed at Canadians or persons in Canada

TOP SECRET

s.15(1) - DEF

IP Profiling Analytics & Mission Impacts

[redacted]

Tradecraft Developer
CSEC – Network Analysis Centre

[redacted]

May 10, 2012

SIGINT

Canadä

TOP SECRET

[redacted]

s.15(1) - DEF

Example IP Profile Problem

- Target appears on IP address, wish to understand network context more fully

- Example Quova look-up & response for [redacted]
  - Lat. 60.00 Long: -95.00 (in frozen tundra W. of Hudson Bay)
  - City: unknown
  - Country: Canada,
  - Operator: Bell Canada, Sympatico

- Issues with IP look-up data:
  - is it actually revealing, or is it opaque
  - is the data even current, or is it out-of-date
  - was the data ever accurate in the first place

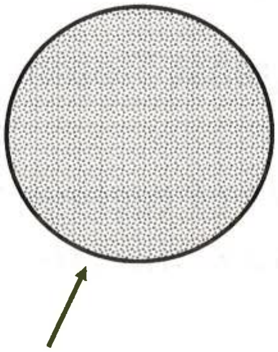
[redacted] [redacted]

Objectives

- Develop new analytics to provide richer contextual data about a network address
- Apply analytics against Tipping & Cueing objectives
- Build upon artefact of techniques to develop new needle-in-a-haystack analytic – contact chaining across air-gaps

Analytic Concept – Start with Travel Node

Begin with *single* seed Wi-Fi IP address of intl. airport



Assemble set of user IDs seen on network address over two weeks

Profiling Travel Nodes – Next Step

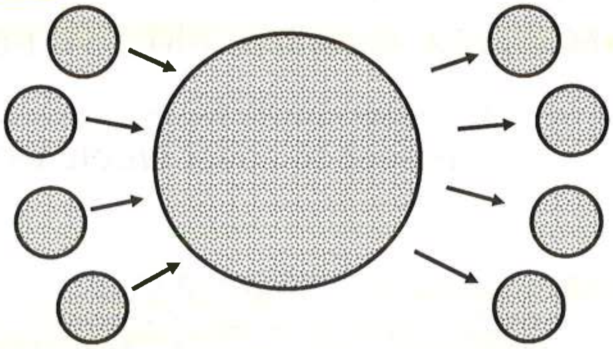
Follow IDs backward and forward in recent time

Earlier IP clusters of:

- local hotels
- domestic airports
- local transportation hubs
- local internet cafes
- etc.

Later IP clusters of:

- other intl. airports
- domestic airports
- major intl. hotels
- etc.

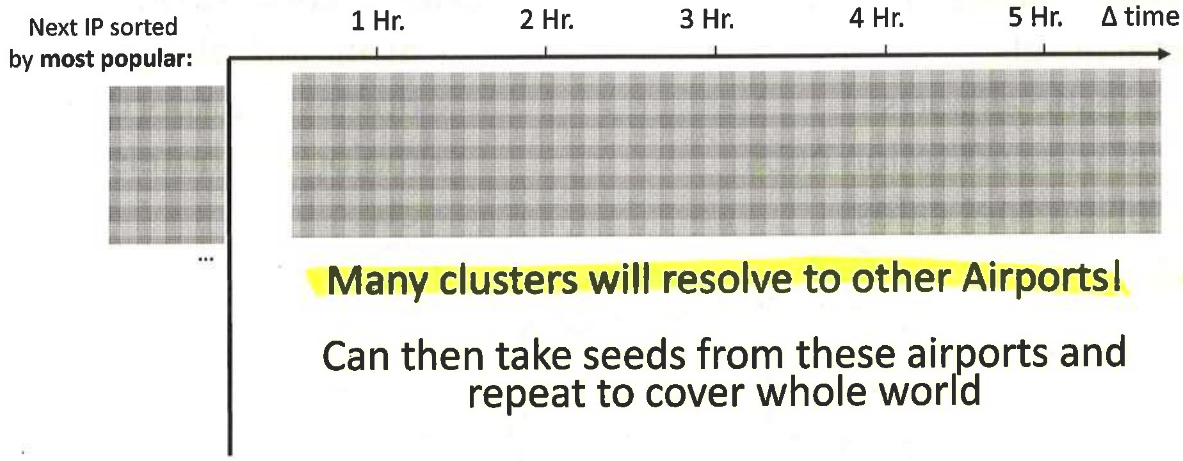


[redacted]

s.15(1) - DEF

IP Hopping Forward in Time

Follow IDs forward in time to
next IP & note delta time



[redacted]

[redacted]

Many clusters will resolve to other Airports!

Can then take seeds from these airports and repeat to cover whole world

Ditto for going backward in time, can uncover roaming infrastructure of host city: hotels, conference centers, Wi-Fi hotspots etc.

[redacted]

[redacted]

Data Reality

- The analytic produced excellent profiles, but was more complex than initial concept suggests

- Data had limited aperture – Canadian Special Source
  - major CDN ISPs team with US email majors, losing travel coverage

- Behaviour at airports
  - little lingering on arrival; arrivals using phones, not WiFi
  - still, some Wi-Fi use when waiting for connecting flight/baggage
  - different terminals: domestic/international; also private lounges

- Very many airports and hotels served by large Boingo private network
  - not seen in aperture; traffic seems to return via local Akamai node

TOP SECRET

[redacted]

s.15(1) - DEF

Tradecraft Development Data Set

- Have two weeks worth of ID-IP data from Canadian Special Source [redacted]

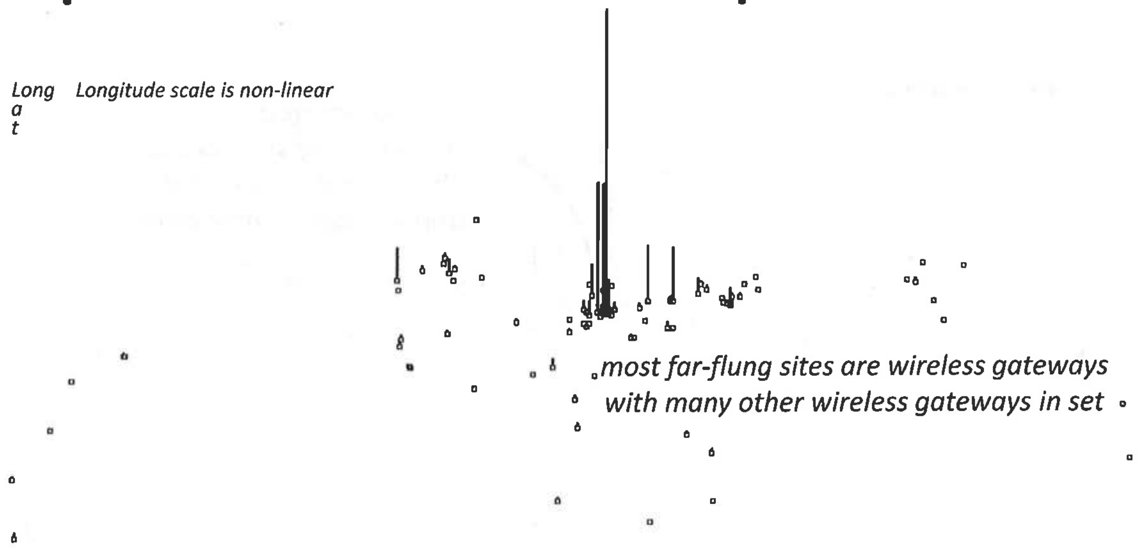
- Had program access to Quova dataset connecting into Atlas database

- Had seed knowledge of a single Canadian Airport WiFi IP address

[redacted]

TOP SECRET

Hop Geo Profile From CDN Airport Intl. Terminal



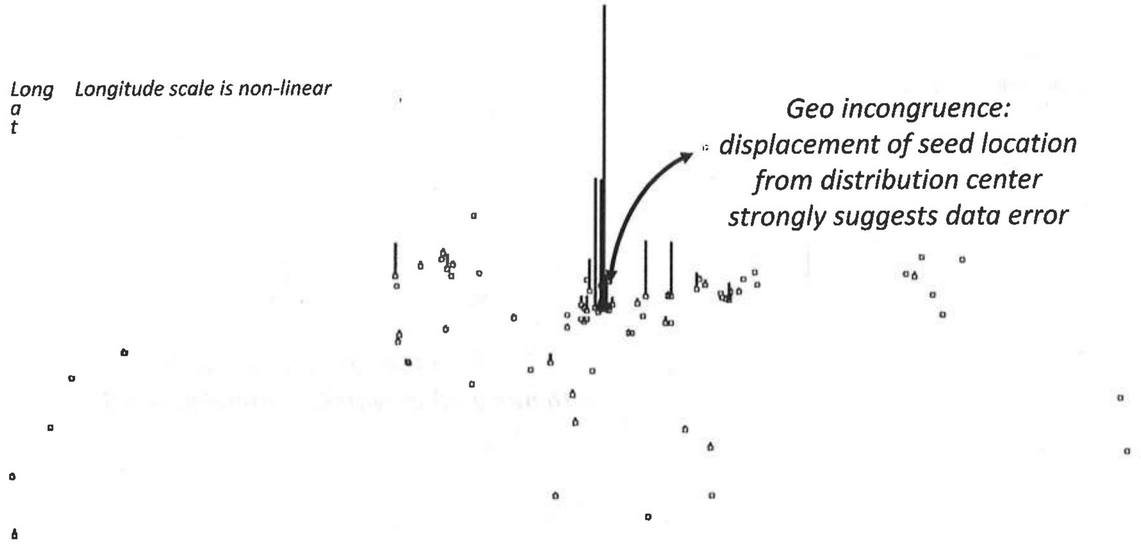
most far-flung sites are wireless gateways with many other wireless gateways in set

Profiled/seed IP location: □ Square = geographic location

Hopped-to IP location: ⍊ Line height = numbers of unique hopped-to IPs at location

Plot of where else IDs seen at seed IP have been seen in two weeks
Plot shows most hopped to IPs are nearby - confirming reported seed geo data

Effect of Invalid Geo Information



Longitude scale is non-linear

Geo incongruence: displacement of seed location from distribution center strongly suggests data error

Profiled/seed IP location: □ Square = geographic location

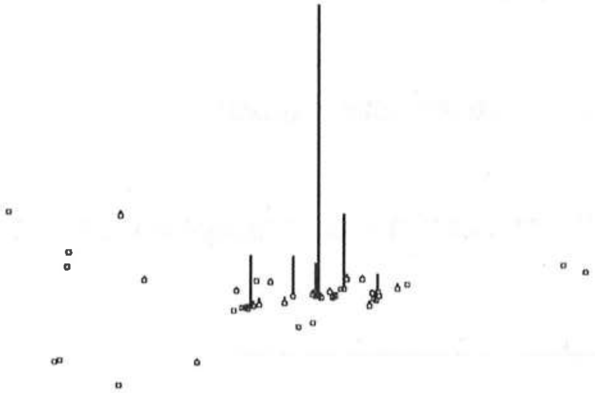
Hopped-to IP location: Line height = numbers of unique hopped-to IPs at location

Effect of invalid seed geo information readily apparent

Hop-Out Destinations Seen

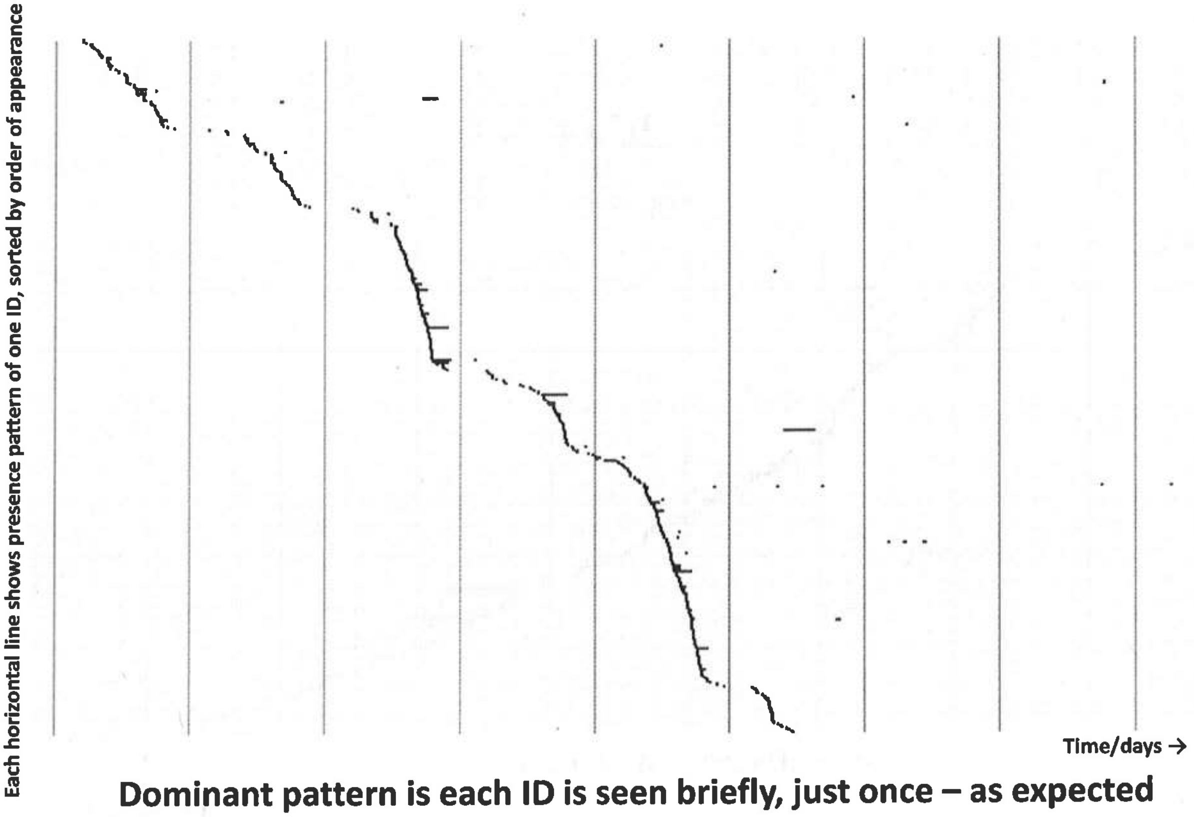
- Other domestic airports
- Other terminals, lounges, transport hubs
- Hotels in many cities
- Mobile gateways in many cities
- Etc.

“Discovered” Other CDN Airport IP



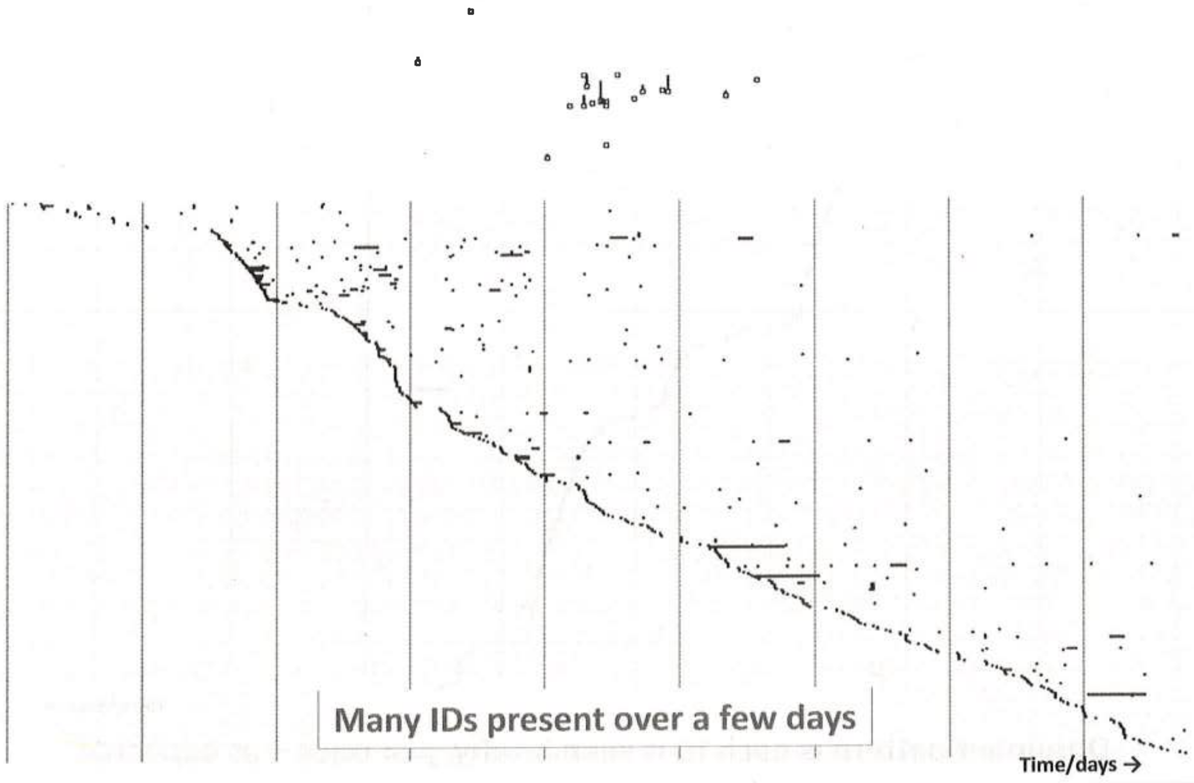
- Domestic terminal
- Closeness of majority of hopped-to IPs confirms geo data
- But, domestic airport can also look like a busy hotel ...

IDs Presence Profile at “Discovered” Airport



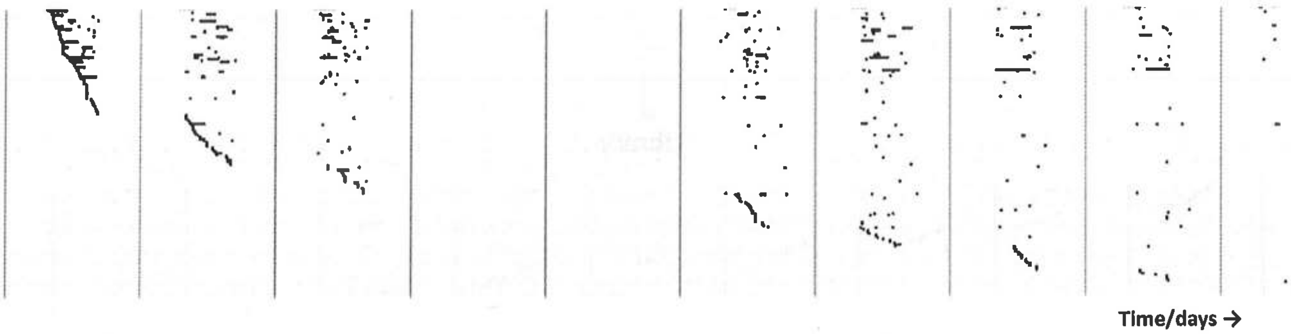
Dominant pattern is each ID is seen briefly, just once – as expected

Profiles of Discovered Hotel



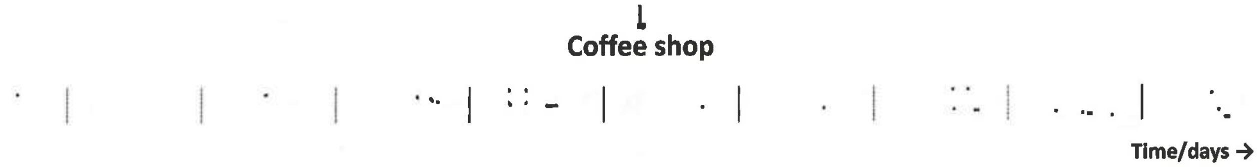
Many IDs present over a few days

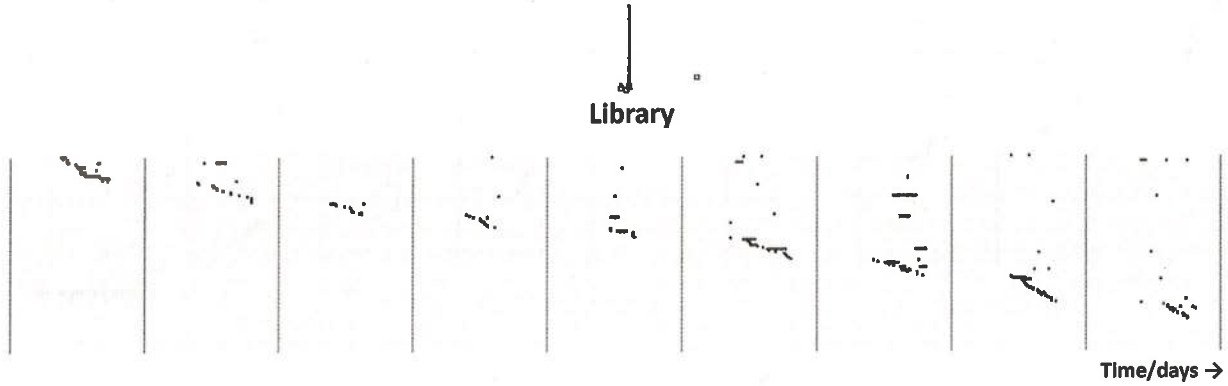
Profiles of Discovered Enterprise



Regular temporal presence (M-F) with local geographic span
Contrasts well against travel/roaming nodes

Discovered Coffee Shop, Library

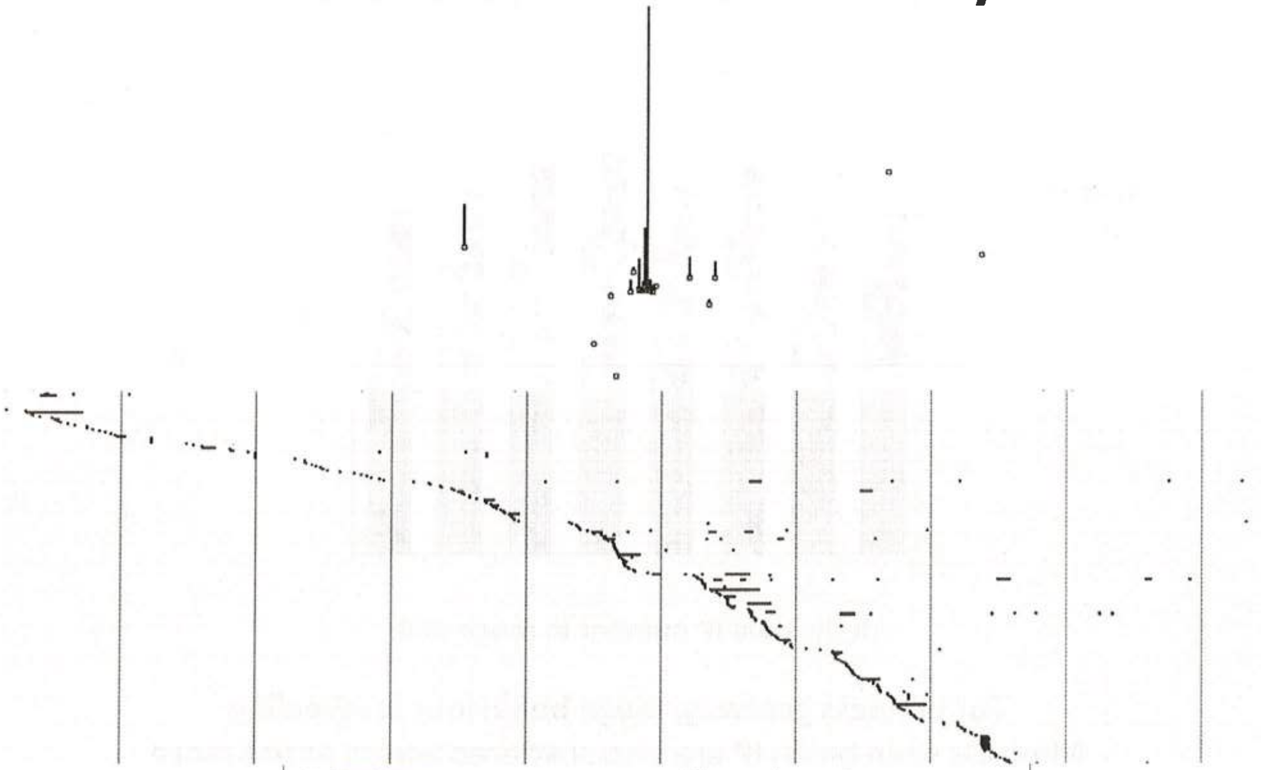




Similar patterns of mixed temporal & local geographic presence

[redacted]

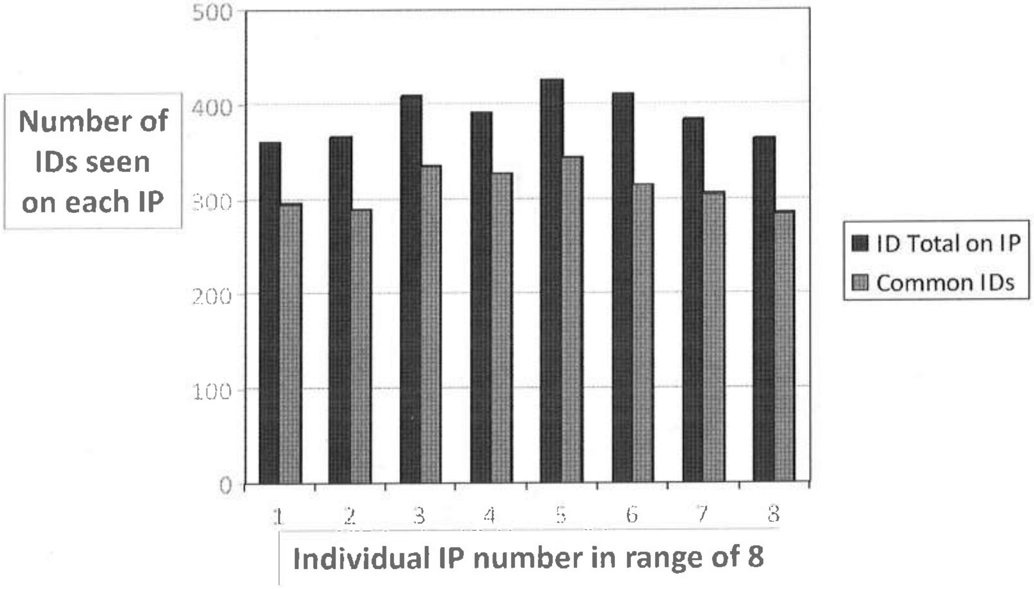
Discovered Wireless Gateway



Wireless gateway not unlike a hotel, except ...

[redacted]

Partial Range Profile of Wireless Gateway



For wireless gateway, range behaviour is revealing
Most IDs seen on an IP are also scattered across entire range
ID totals & traffic across full range is very high

Mission Impact of IP Profiling

- Tipping and Cueing Task Force (TCTF)
  - a 5-Eyes effort to enable the SIGINT system to provide real-time alerts of events of interest
  - alert to: target country location changes, webmail logins with time-limited cookies etc.

- Targets/Enemies still target air travel and hotels
  - airlines: shoe/underwear/printer bombs …
  - hotels: Mumbai, Kabul, Jakarta, Amman, Islamabad, Egyptian Sinai …

- Analytic can hop-sweep through IP address space to identify set of IP addresses for hotels and airports
  - ***detecting target presence within set will trigger an urgent alert***
  - aim to productize analytics to reliably produce set of IPs for alerting

IP Profiling Summary

- Different categories of IP ownership/use show distinct characteristics
  - airports, hotels, coffee shops, enterprises, wireless gateways etc.
  - clear characteristics enable formal modeling developments
  - clear identification of hotels and airports enables critical Tipping & Cueing tradecraft
- Geo-hop profile can confirm/refute IP geo look-up information
  - later could fold-in time deltas for enhanced modeling
- Can "sweep" a region/city for roaming access points to IP networks
  - ***leads to a new needle-in-a-haystack analytic ...***

[redacted]

Tradecraft Problem Statement

- A kidnapper based in a rural area travels to an urban area to make ransom calls
  - can't risk bringing attention to low-population rural area
  - won't use phone for any other comms (or uses payphones ...)

- Assumption: He has another device that accesses IP networks from public access points
  - having a device isn't necessary, could use internet cafes, libraries etc.
  - he is also assumed to use IP access around the time of ransom calls

- Question: Knowing the time of the ransom calls can we discover the kidnapper's IP ID/device
  - "contact chain" across air-gap (not a correlation of selectors)

[redacted]

Solution Outline

- With earlier IP profiling analytics, we can "sweep" a city/region to discover and determine public accesses

- We can then select which IP network IDs are seen as active in all times surrounding the known ransom calls
  - reduce set to a shortlist

- Then we examine the reduced set of IP network IDs and eliminate baseline heavy users in the area that fall into the set intersection just because they are always active
  - that is, eliminate those that are highly active outside the times of the ransom calls
  - ***hopefully leaves only the one needle from the haystack***

[redacted]

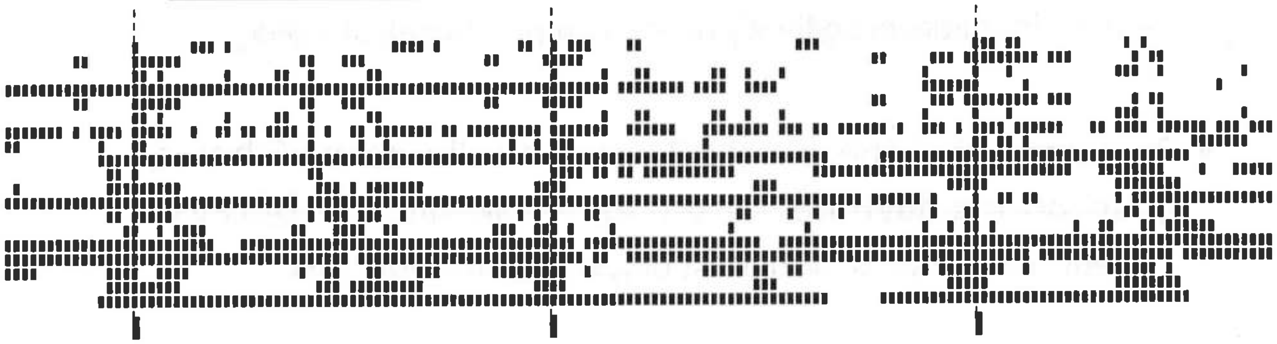
First Proof-of-Concept

- Swept a modest size city and discovered two high traffic public access ranges with >300,000 active IDs over 2 weeks
  - – used for initial expediency due to computational intensity
- Presumed that there were 3 ransom calls, each 50 hours apart during daytime, looked for IDs within 1 Hr of calls
  - – reduce large set to a shortlist of just 19 IP network IDs
- Examined activity level of 19 IP network IDs – how many presences each had in 1 Hr slots over two weeks
  - – main worry as the computation was running: there would be a lot of IDs that showed just a handful of appearances: e.g. 3, 4, 5 instances

[redacted] [redacted]

ID Presence of Shortlist

Each horizontal line shows presence of ID over time/hour-slots



Postulated presence of kidnapper/target

Happy result: least active ID had appearances in 40 hour-slots!
Thus could eliminate all, leaving just the kidnapper (if he was there)

[redacted]

s.15(1) - DEF
s.15(1) - IA

Big-Data Computational Challenge

- All the previous analytics, while successful experimentally, ran much too slowly to allow for practical productization

- CARE: Collaborative Analytics Research Environment
  - a big-data system being trialed at CSEC [redacted]
  - non-extraordinary hardware
  - minimal impedance between memory, storage and processors
  - highly optimized, in-memory database capabilities
  - columnar storage, high performance vector functional runtime
  - powerful, [redacted] challenging [redacted] language (derived from APL)

- Result of first experiments with CARE: game-changing
  - run-time for hop-profiles reduced from 2+ Hrs to several seconds
  - ***allows for tradecraft to be profitably productized***

[redacted] [redacted]

Overall Summary

- **IP profiling showing terrific value**
  - – significant analytic asset for IP networks and target mobility
  - – enables critical capability within Tipping & Cueing Task force
  - – working to productize on powerful new computational platform
  - – broader SSO accesses/apertures coming online at CSEC
  - – look to formalize models & fold-in timing deltas

- **A new needle-in-a-haystack analytic is viable:** contact chaining across air-gaps
  - – enabled by sweep capability of IP profiling
  - – should test further to understand robustness with respect to loosening assumptions of target behaviour
  - – beyond kidnapping, tradecraft could also be used for any target that makes occasional forays into other cities/regions

67

Page~~s~~ ~~66 to / à 69~~

is a ~~are~~ duplicate~~s~~

sont des duplicatas

s.15(1) - DEF

TOP SECRET

[redacted]

[redacted] Tradecraft Studio Example

[redacted]

Possible route for productizing analytics

[redacted] [redacted]