SECRET

IPOC

- Roles and Responsibilities
- Policy Structure
- Key Terms/Concepts
- Relationships and Sharing

1

Part B of the Mandate

"to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada;"
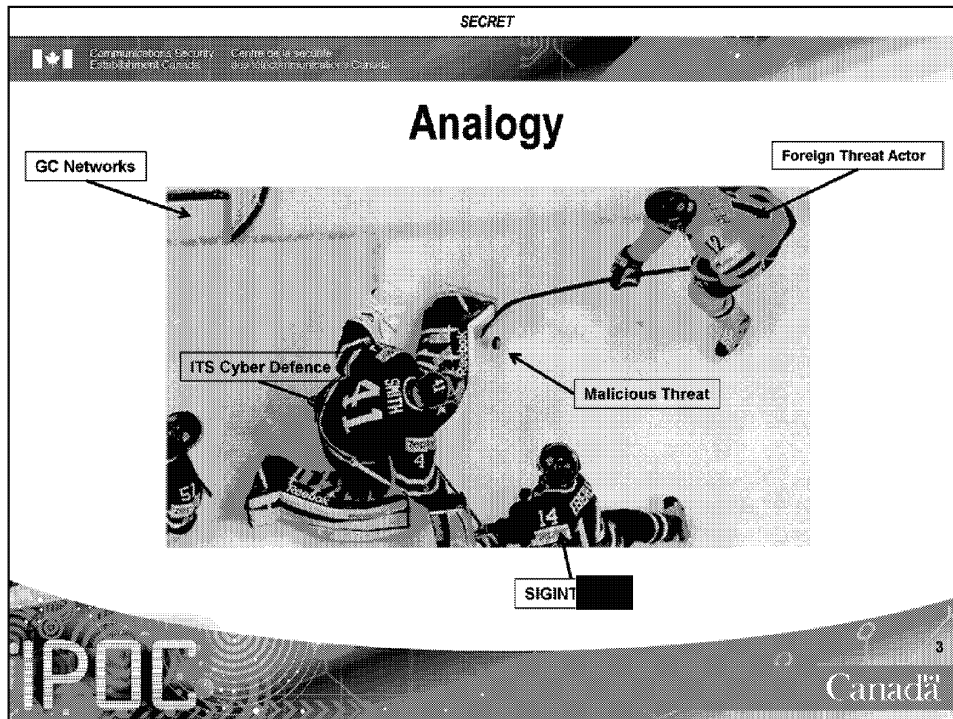
ITS Cyber Defence is like being the goalie in a hockey match. Our role is to keep the puck out of our net as it comes to us. We don't focus on the opposing player, SIGINT handles that, our only concern is keeping our net free from pucks.

Here's the problem though, we bring out own refs and abide by the rulebook. Unfortunately, the ref doesn't look at the other team and they don't have a rule book... They are always on the power-play and have more than one puck on the ice at time.

So we try out best to stop the puck, but it's inevitable that some end up in the net. And if we focus our attention cleaning up our filled net, more pucks just get in...

3

Communications Security   Centre de la sécurité
Establishment Canada   des télécommunications Canada

IPOC Mission

The purpose of ITS Policy Oversight and
Compliance (IPOC) is to enable the
development and delivery of IT Security
cyber defence operations to external
federal institutions by coordinating
associated governance, compliance, policy
and legal requirements.

IPOC   Canada

4

ITS Policy Structure

* OPS-1
* OPS-1-14
* OPS-1-15
* 6 ITSOIs
  - Data Handling
  - Data Access and Sharing
  - Report Management
  - Data Querying
  - Tool deployments (in draft)
  - Compliance Monitoring

5

Definition of PC

"A recognized private communication includes a recognized private communication in whole or in part, or metadata associated with a recognized private communication that can identify one or both communicants or the communication itself."

SECRET

Idents in ITS

- There are only 3
  - Email addresses
  - IP addresses
  - Domain names
- CII can get complicated
  - Email addresses are often spoofed
  - .ca domains resolve to foreign IPs
  - Legitimate company names are registered by foreign threat actors

7

Types of Operations

- MA
- Non-MA

AGC0211

8

Data

- Data
- Raw Data
- Used and Retained Data
- MA vs Non-MA
- Classification of ITS reports

9

SECRET

Sharing

- Sharing with SIGINT
- Triaging
- Sharing with the 5-eyes (Relevant and Essential)
- Reporting domestically

IPOC

SECRET

Closing Thoughts

- Many cyber players in Canada (Public Safety, SSC, DND, CSIS, etc.)
- ITS / SIGINT collaboration in the 5-eyes community (e.g. ████████████
- Working and sharing with Industry is extremely important (lessons learned from ████████████

11

SECRET

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Policy Activity

- 4 examples to discuss 'directed at Canadians' in the context of ITS activities:

1.

2.

3.

4.

IPOC

Canada

12

Questions?