Federal Policing National Security

Foreign Actor Interference Team

Royal Canadian Mounted Police / Gendarmerie royale du Canada

July 2021

Canada

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Who is your FPNS FAIT?

- A/OIC
- A/S/Sgt
- A/Sgt
- Sgt
- Sgt

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Why was FAIT created?

- The RCMP's National Security Program has a clear role to play in protecting Canada and Canadians from foreign actor interference
- FPNS recognized that foreign state actors are targeting Canada to advance their own interests and expect that FAI investigations will increase in the immediate future
- The RCMP Federal Strategic Plan 2020-2023 specifically identified foreign interference activities as a priority under the scope of its core National Security mandate
- FPNS recognized that foreign actor interference may cause severe political repercussions influenced by national or international interests

National Security Program

Mandate

The National Security Program retains primary responsibility in the investigation of the following national security offences:

RCMP Operations Manual 12.2.2.1.3

Threats to the security of Canada as defined in sec 2, Canadian Security Intelligence Act.

What is Foreign Actor Interference?

- Foreign Actor Interference (FAI) is any ***illegal*** activity conducted at the direction or for the benefit of a foreign entity which targets Canadian interests, or interferes in Canadian society and threatens Canada's national security.

What does FAIT do?

Our Mission

Enable the National Security Program to prevent, disrupt, and prosecute Foreign Actor Interference.

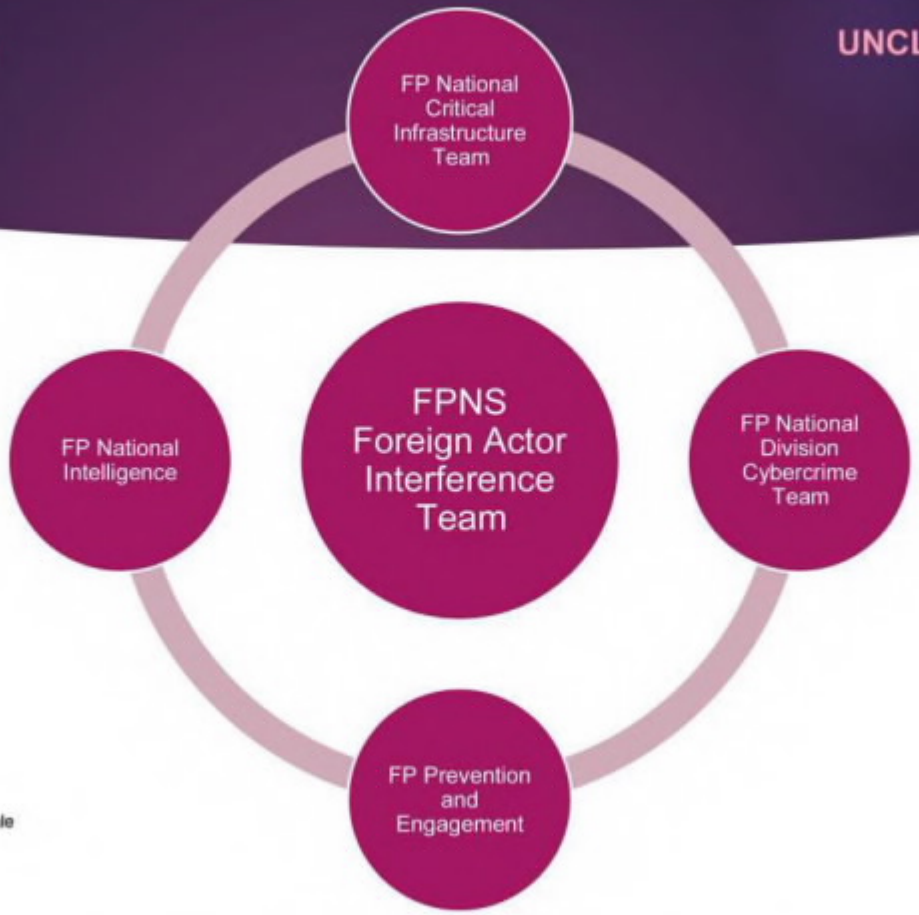
How do we achieve our mission?

The FPNS FAIT review, co-ordinate, advise, and provide governance on matters of National Security related to ***illegal*** activities conducted at the direction or for the benefit of a foreign entity.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

How?



Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Common FAI Activities under the CCC

- Theft of Technology
- Theft of Intellectual Property or Theft of Trade Secrets
- Theft of Data
- Breach of Trust
- Mischief
- Fraud

Common FAI Activities Cont'd

- Intimidation
- Criminal Harassment
- Interception of Communications

Threats of violence by state representatives or their proxies, illegal interception of communications or following or monitoring a person are examples of occurrences being reported by persons attending pro-democracy demonstrations, people speaking publicly against certain organizations or governments, and citizens of other countries who criticize their governments.

Section 391 *Criminal Code (New)*

Section 391 states that "[e]veryone commits an offence who, by deceit, falsehood or other fraudulent means, knowingly obtains a trade secret or communicates or makes available a trade secret."

A trade secret is defined as information that (a) is not generally known in the trade or business that may use that information, (b) has economic value for not being generally known, and (c) is subject to reasonable efforts to maintain its secrecy.

Security of Information Act

- Communicating safeguarded information
- Breach of trust in respect of safeguarded information
- Use of trade secret for the benefit of foreign economic entity
- Foreign-influenced or Terrorist-influenced threats or Violence
- Preparatory Acts

Public Servant Inventions Act

- **Duties of inventor**

4(1) Every public servant who makes an invention

(a) Shall inform the appropriate minister of the invention and shall provide the minister with such information and documents with respect thereto as the minister requires

(b) Shall not file outside Canada an application for a patent in respect of the invention without the written consent of the appropriate minister; and

(c) Shall, in any application in Canada for a patent in respect of the invention, disclose in this application that he is a public servant

s. 39 - Cabinet Confidence

Contact FPNS FAIT

A/OIC
Office:
Mobile
Email: @rcmp-grc.gc.ca

A/S/Sgt
Office:
Mobile
Email: @rcmp-grc.gc.ca

Sgt
Office:
Mobile:
Email: @rcmp-grc.gc.ca

A/Sgt
Office:
Mobile
Email: @rcmp-grc.gc.ca

Sgt
Office:
Mobile
Email: @rcmp-grc.gc.ca

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Slide Notes

Slide 3:
There will be a contact list on a separate slide at the end of this presentation.

The FAIT falls under the supervision of Insp [redacted] the Acting Director of FPNS Ops 1. According to the most recent organization chart, the FAIT is considered Review Team #3 and deals solely with FAI files from across the country. The FAIT is the only team that is not based on any specific region. It has the responsibility to oversee FAI files in all of Canada in order to have a better understanding of the FAI threat picture on a national scale.

FAIT is trying to acquire two full time analysts who would be dedicated solely to the FAIT. Whenever possible, FAIT has been working with specific analysts with expertise in certain countries.

Slide 4:
Review, co-ordinate, advise and provide governance on matters of National Security related to illegal activities conducted at the direction or for the benefit of a foreign entity.

The RCMP's authority to investigate FAI is covered by Section 2 of the Canadian Security Intelligence Service Act

Develop subject matter experts within FPNS for various regions/countries of the world and their political agendas.

Slide 5:
Section 2 of the CSIS Act states that threats to the security of Canada may be:

espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person or
c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state.

Slide 6:

It is important to make a distinction between the fundamental freedoms of expression, thought, belief, and opinion, including the press and media. Everyone has the right to hold opinions without interference and is protected by Section 2 of the Canadian Charter of Rights and Freedoms (there are "reasonable" limits to freedom of expression, most commonly hate speech, obscenity, and defamation). However, foreign actor interference is purposely covert, malign, clandestine and deceptive. It is directed at Canadians, or residents of Canada, or Canadian institutions to advance foreign strategic interests.

Slide 7:

Foreign Actor Interference (FAI) is illegal activity which targets Canadian interests, or interferes in Canadian society and threatens Canada's national security. These threats to national security involve covert, coercive and clandestine efforts by, or for, a foreign actor to advance their own strategic interests to the detriment of Canada. Foreign actors engage in a broad range of activities which contravene Canadian Law, including but not limited to: hacking and cyberattacks; criminal intimidation of diaspora communities; manipulation of traditional and social media; clandestine proliferation efforts; theft of government (Federal or Provincial) protected information, and trade secrets. FAI can be conducted by representatives of the state (e.g. intelligence or police agents) or by proxies (e.g. individuals or groups of people) who are directed to conduct illegal activity

Slide 8:

The RCMP's National Security Program investigates threats to the security of Canada by upholding various laws for the purpose of preventing offences from happening and bringing to justice those who contravene Canadian legislation. FAIT works collaboratively with several other units when an incident or investigation involves hostile state actors depending on the nature of the threat.

NCIT – 10 Sectors: Energy and Utilities
Finance
Food
Government
Health
Information and Communication Technology
Manufacturing
Safety Transportation
Water

Cyber - Cybercrime is a broad term that captures both crimes where technology is the primary target and those where technology is a significant enabler in more traditional crimes.

The RCMP Cybercrime Teams take on cybercrime investigations that involve Technology-as-Target, but may assist in certain major cyber-enabled (Technology-as-Instrument) cases.

Cybercrime that involves "Technology-as-Target" are those criminal offences targeting computers and other information technologies, such as those involving the unauthorized use of computers CC 342.1 or mischief in relation to data CC 430 (1). Examples include data breaches, DDOS attacks, hacking activities, providing or selling cybercrime tools (cybercrime as a service), and ransomware.

Prevention and Engagement – public engagement and outreach, relationships that will enable community members to report intimidation tactics. Passenger protect

FPNI – threat picture

Slide 9:

There are a broad range of offences within the Criminal Code that can be brought against individuals to disrupt and/or prosecute foreign actor interference. Several other pieces of legislation should also be considered when investigating FAI.

If the individual is working for the Government of Canada and has a security clearance, the Security of Information Act applies and carries severe penalties.

Other legislation should also be considered depending on the offence and the type of theft, for example: Defence Production Act, Transportation of Dangerous Goods Act, Human Pathogens and Toxins Act,

FPNS has seen theft of agricultural products, research and technology like grain, soy, and covid 19 vaccines which are threatened especially from hostile state actors at universities, educational facilities, and research labs.

FPNS is usually notified of these types of complaints through Departmental Security Officers who are usually at some stage in their internal investigation process.

Theft of information / Technology is a type of Foreign Actor Interference investigation which are incidents of agents or proxies of a foreign entity illegally obtaining or the attempting to obtain information or technology that is protected by the government of Canada or is a trade secret and that obtainment is for a purpose of increasing the capacity of the foreign entity.

Examples of police investigations which the RCMP National Security Program have monitored for a foreign entity involvement was a report of a theft of students and professor's passwords from a university data base; and the theft of protected data by a contracted employees working at a government facility.
The thefts may be at the direction or in support of a foreign state because the data taken may have:
provided access points to obtain other protected data,
provided highly valued research information not publically accessible,
access to information may which may be of dual use meaning the information taken may be used to creating or advancing weapons.

Targeting Canadian Industry
Companies leading in innovation, research & development, and cutting edge technology are attractive targets
Insider threats can weaken or destroy public trust in a company, threatening its financial foundation
Covertly obtaining sensitive technology or information from another organization can cause significant damage to Canadian interests

Targets Include:
Educational Institutes
Academics, Scientists, Researchers, Experts, Business Figures and Professionals

Slide 10:
Engage targets to coerce, co-opt, or recruit persons:

Ukraine International Airlines Flight 752 (PS752) – the flight was shot down by the Iranian Islamic Revolutionary Guards Corp (IRGC) and all 176 passengers and crew were killed. The crash was the largest loss of Canadian lives in aviation since the 1985 bombing of Air India Flight 182. Family members in Canada who have criticized Iran's government after losing their loved ones in the downing of Ukraine International Airlines Flight 752 say they're being targeted with threats and intimidation. Iranian Government officials visiting family members of the deceased and threatening them if they continue talking and speaking out. They also threaten family members who remain in Iran.

China - The PRC's National Intelligence Law compels all Chinese entities and citizens inside and outside of China to cooperate with the Chinese government on national security issues. The four basic concepts of China's national security law are subversion, secession, terrorism, and collusion with foreign forces. The diverse range of activities undertaken by the PRC presents challenges to law enforcement because, while some aspects are clearly illegal, many other activities are in the "grey" zone of not being strictly illegal, and do not align with traditional foreign espionage acts.

Are individuals acting of their own free will or are they being intimidated/harassed to perform specific actions.

Slide 11:

Note: Unlike some other countries, Canada does not have any criminal intellectual property laws. However, section 391 of the Criminal Code was recently amended to criminalize the misappropriation of trade secrets. As a work around to the lack of intellectual property offences, investigators should consider the use of fraud, theft of data, theft of technology under the Criminal Code and/or SOAI offences such as communicating safeguarded information, breach of trust etc. If the offender is a public servant and the information was used in a patent, The Public Servant Inventions Act could be considered.

Companies must ensure both that they have taken reasonable steps to protect their trade secrets, and that they have internal measures in place to avoid liability for the theft of another person's trade secret, whether this is in the context of new employees joining the organization or in the context of business negotiations, during which confidential information of another organization may become known.

Canadian courts will likely consider the extent to which the owner took to advise the recipients of the trade secrets that the information was confidential and limited access to the information.

"Everyone" can include both individuals and organizations

Slide 12:

Communications with Foreign Entities or Terrorist Groups
Communicating safeguarded information
16 (1) Every person commits an offence who, without lawful authority, communicates to a foreign entity or to a terrorist group information that the Government of Canada or of a province is taking measures to safeguard if
(a) the person believes, or is reckless as to whether, the information is information that the Government of Canada or of a province is taking measures to safeguard; and

(b) the person intends, by communicating the information, to increase the capacity of a foreign entity or a terrorist group to harm Canadian interests or is reckless as to whether the communication of the information is likely to increase the capacity of a foreign entity or a terrorist group to harm Canadian interests.

Communicating safeguarded information

(2) Every person commits an offence who, intentionally and without lawful authority, communicates to a foreign entity or to a terrorist group information that the Government of Canada or of a province is taking measures to safeguard if

(a) the person believes, or is reckless as to whether, the information is information that the Government of Canada or of a province is taking measures to safeguard; and

(b) harm to Canadian interests results.

Punishment

(3) Every person who commits an offence under subsection (1) or (2) is guilty of an indictable offence and is liable to imprisonment for life.

2001, c. 41, s. 29

Communicating special operational information

17 (1) Every person commits an offence who, intentionally and without lawful authority, communicates special operational information to a foreign entity or to a terrorist group if the person believes, or is reckless as to whether, the information is special operational information.

Punishment

(2) Every person who commits an offence under subsection (1) is guilty of an indictable offence and is liable to imprisonment for life.

2001, c. 41, s. 29

Breach of trust in respect of safeguarded information

18 (1) Every person with a security clearance given by the Government of Canada commits an offence who, intentionally and without lawful authority, communicates, or agrees to communicate, to a foreign entity or to a terrorist group any information that is of a type that the Government of Canada is taking measures to safeguard.

Punishment

(2) Every person who commits an offence under subsection (1) is guilty of an indictable offence and is liable to imprisonment for a term of not more than two years.

2001, c. 41, s. 29

Economic Espionage

Use of trade secret for the benefit of foreign economic entity

19 (1) Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right and to the detriment of Canada's economic interests, international relations or national defence or national security

(a) communicates a trade secret to another person, group or organization; or
(b) obtains, retains, alters or destroys a trade secret.
Punishment
(2) Every person who commits an offence under subsection (1) is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.
Defence
(3) A person is not guilty of an offence under subsection (1) if the trade secret was
(a) obtained by independent development or by reason only of reverse engineering; or
(b) acquired in the course of the person's work and is of such a character that its acquisition amounts to no more than an enhancement of that person's personal knowledge, skill or expertise.
Meaning of trade secret
(4) For the purpose of this section, trade secret means any information, including a formula, pattern, compilation, program, method, technique, process, negotiation position or strategy or any information contained or embodied in a product, device or mechanism that
(a) is or may be used in a trade or business;
(b) is not generally known in that trade or business;
(c) has economic value from not being generally known; and
(d) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Foreign-influenced or Terrorist-influenced Threats or Violence
Threats or violence
20 (1) Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign entity or a terrorist group, induces or attempts to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done
(a) that is for the purpose of increasing the capacity of a foreign entity or a terrorist group to harm Canadian interests; or
(b) that is reasonably likely to harm Canadian interests.
Application
(2) A person commits an offence under subsection (1) whether or not the threat, accusation, menace or violence occurred in Canada.
Punishment
(3) Every person who commits an offence under subsection (1) is guilty of an indictable offence and is liable to imprisonment for life.

Harbouring or Concealing
Concealing person who carried out offence

21 (1) Every person who, for the purpose of enabling or facilitating an offence under this Act, knowingly harbours or conceals a person whom they know to be a person who has committed an offence under this Act, is guilty of an indictable offence and liable to imprisonment
(a) for a term of not more than 14 years, if the person who is harboured or concealed committed an offence under this Act for which that person is liable to imprisonment for life; and
(b) for a term of not more than 10 years, if the person who is harboured or concealed committed an offence under this Act for which that person is liable to any other punishment.
Concealing person who is likely to carry out offence
(2) Every person who, for the purpose of enabling or facilitating an offence under this Act, knowingly harbours or conceals any person whom he or she knows to be a person who is likely to carry out an offence under this Act, is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years.

Preparatory Acts
Preparatory acts
22 (1) Every person commits an offence who, for the purpose of committing an offence under subsection 16(1) or (2), 17(1), 19(1) or 20(1), does anything that is specifically directed towards or specifically done in preparation of the commission of the offence, including
(a) entering Canada at the direction of or for the benefit of a foreign entity, a terrorist group or a foreign economic entity;
(b) obtaining, retaining or gaining access to any information;
(c) knowingly communicating to a foreign entity, a terrorist group or a foreign economic entity the person's willingness to commit the offence;
(d) at the direction of, for the benefit of or in association with a foreign entity, a terrorist group or a foreign economic entity, asking a person to commit the offence; and
(e) possessing any device, apparatus or software useful for concealing the content of information or for surreptitiously communicating, obtaining or retaining information.
Punishment
(2) Every person who commits an offence under subsection (1) is guilty of an indictable offence and is liable to imprisonment for a term of not more than two years.

Slide 13:
This is with respect to patents

Slide 14:

In consultation with Operations Research and the National Critical Infrastructure Team, FPNS has recommended substantive amendments to SOIA to provide the Government of Canada with the ability to prosecute FAI activities prejudicial to the safety of Canada.

There could be an entire slide presentation on the proposed amendments itself, however this is still in the working phase. The proposed amendments were modeled after existing US and Australian legislation.