SECRET

National Security Operational Threat Picture

Foreign Actor Interference - People's Republic of China

Federal Policing National Security
FI Operational Coordination Meeting
2023-07-05

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Note:

- This presentation is based on the dataset analyzed so far by FPNS-OA.
- The information within this presentation is subject to change as the data is further analyzed and new information becomes available. This presentation is based on information available to date.
- Data, charts and case studies may contain caveated and/or third-party information derived from the RCMP's investigative holdings and/or Canadian police databases.

Foreign Actor Interference – Target Areas

SECRET

Target Areas in Canada:

Economic Integrity	Proliferation	Theft of Intellectual Property	Theft of Protected Information
Critical Infrastructure	Transnational Repression	Disinformation	Democratic Institutions

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

FAI Activity Categories: Target Areas & Effect

SECRET

Economic Integrity

Leveraging Canada's open economy through strategic foreign investment; exports; rights and licenses; and, knowledge with the purpose of gaining influence or advantage over strategic resources, research, technologies and industries. **This degrades Canada's economic integrity.**

- ✓ Foreign Investment: property; assets and infrastructure
- ✓ Catch all

Proliferation

Efforts to procure sensitive, restricted and dual-use technologies and goods which bolster the State actor's military capabilities and strategic advantage. This has **implications for global peace and security.**

- ✓ Weapons of mass destruction (WMD) program development
- ✓ Violations of sanctions

Theft of Intellectual Property

Efforts to gain commercial, academic, scientific and military information, goods and technologies from GoC/private companies, research and academic institutions. **This activity undermines Canada's global competitive edge and prosperity.**

- ✓ Academic espionage
- ✓ Innovative technologies

Theft of Protected Information

Targeted acquisition of information secured from the public, or bound by confidentiality agreements. **This activity threatens Canada's national security & economic integrity.**

- ✓ SOIA and insider threats
- ✓ Trade secrets / Classified information

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

FAI Activity Categories: Target Areas & Effect

SECRET

Transnational Community Repression

Monitoring, intimidating and using violence against Canadian diaspora communities to force cooperation or mute criticisms of regime policies, **represents a threat to Canada's sovereignty and the safety of Canadians.**

- ✓ Assassination, Coercion, Threats, Intimidation & Harassment
- ✓ Renditions and Forced Repatriations

Disinformation

State-sponsored manipulation of information and use of misinformation seeking to influence or to **discredit and erode confidence in Canada's democratic institutions, policies and values.**

- ✓ Use of online platforms and community spaces influence narratives
- ✓ Targeting of elected officials

Democratic Institutions

Interfering in and influencing Canada's democratic processes which **corrodes Canada's democracy and social cohesion**.

- ✓ Corruption of elected officials
- ✓ Cultivation of relationships with key demographics
- ✓ Election interference
- ✓ Placement of individuals in positions of influence

Critical Infrastructure

Exploiting vulnerabilities across all sectors of Canada's critical infrastructure, including Canada's energy sector and Information and Communication technologies.

- ✓ Cyber attacks
- ✓ Supply chains

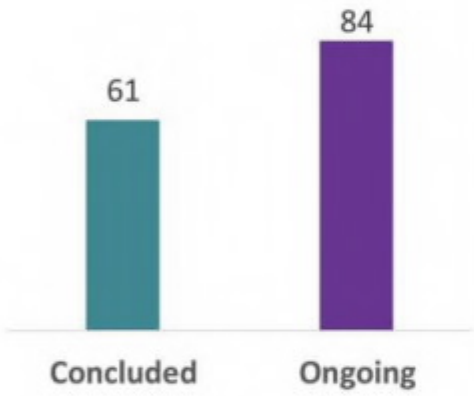
Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

5

FPNS Preliminary Assessment of NS FAI-PRC Files

SECRET



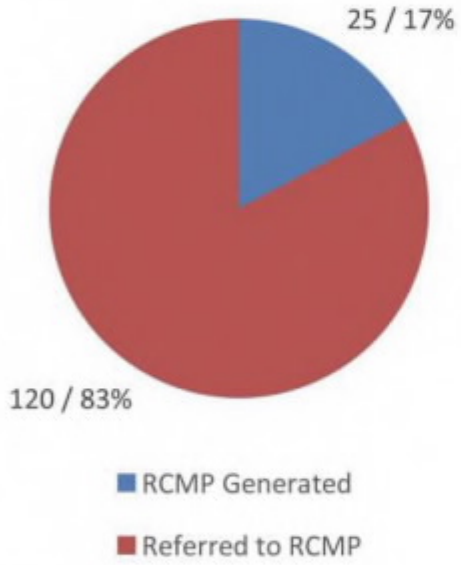
4*	5	2
Individuals convicted since 2011	Individuals currently charged	Charge packages being developed
16 charges total	**13 charges total**	**5 anticipated charges**

145 National Security FAI-PRC related files were reviewed for convictions/charges/charge packages.
Assessment ongoing

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Preliminary Assessment: FAI-PRC Files



Genesis of FAI-PRC Files

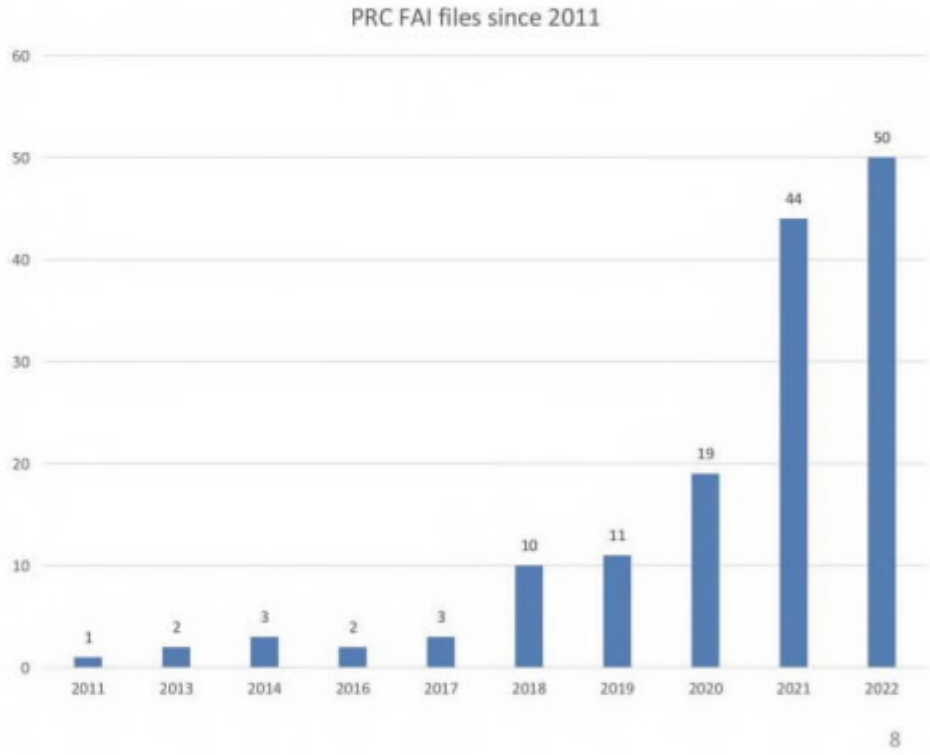
23%	International Law Enforcement
23%	Public complaint/tip
18%	RCMP generated
16%	GoC Department (victim/complainant)– AAFC, PHAC, CSA, CFIA, etc.
10%	Other Canadian Agency – CSIS, FINTRAC, CBSA
5%	Domestic Law Enforcement
1%	Private Company
1%	Academic Institution
3%	International Organization

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

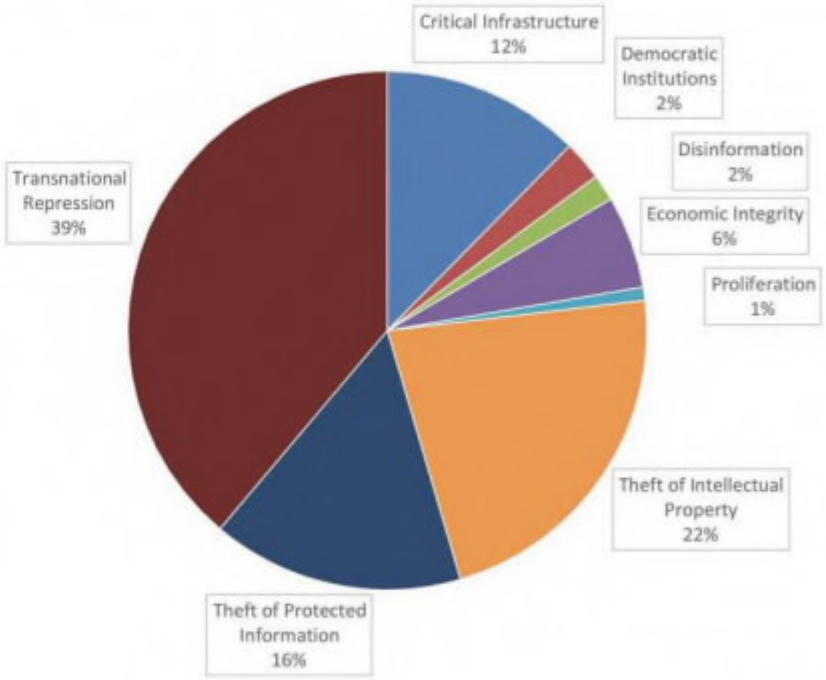
Preliminary Findings: Annual File Counts

- RCMP previously not tracking FAI files.
- Pre-2019, lack of PRC FAI-related reporting and minimal RCMP posture on PRC FAI activities (CSIS primacy in FAI space).
- Notable increase in files in 2018-2019: shift in PRC's strategic plans and an increased threat awareness among Five Eye partners.
- Further increase in 2020 and 2021: partner drive (CSIS,) and likely corresponds with the creation of the FPNS FAI team in 2020, and dedicated resources to triage, assess and act on FAI-related threats.



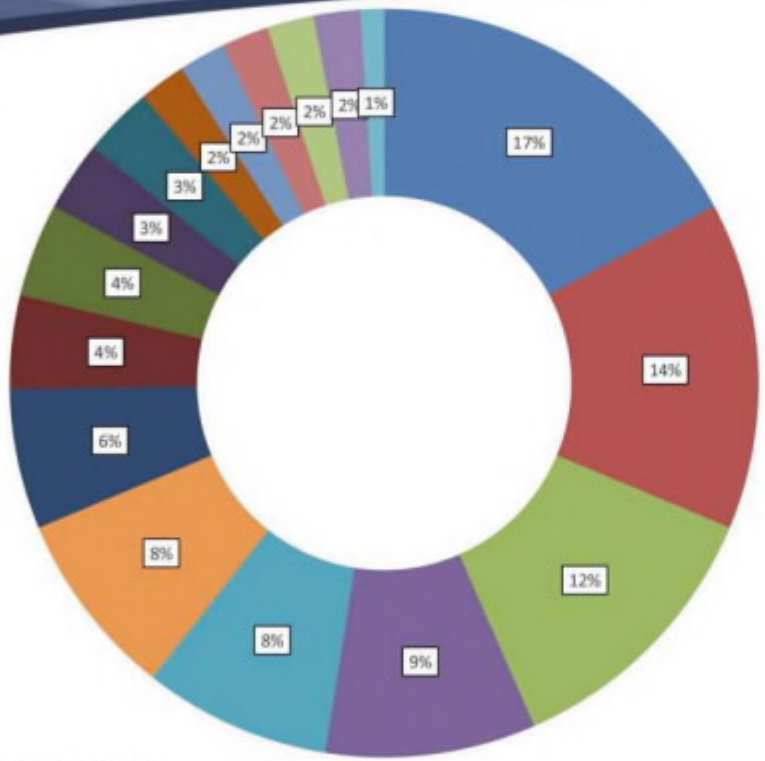
Preliminary Findings: Target Areas

- Two largest target areas of FAI-PRC:
  - Transnational community repression
  - Theft of intellectual property
- Proliferation is likely highly underrepresented.
- Lower counts of economic integrity, disinformation and democratic institutions may reflect the lack of visibility on files held outside of FPNS.
- One file can fall into multiple categories of the target areas.



SECRET

Tactics Techniques and Procedures Observed



- Use of front companies or associations
- Cyber for theft of IP and/or PI
- Threats, violence, intimidation, or coercion of family and associates in Canada and/or the PRC
- Canadian private enterprises as a vehicle for theft of IP and/or PI
- Cyber as a vehicle for repression
- Canadian public enterprises as a vehicle for theft of IP and/or PI
- Strategic Placement (Insider Threat)
- Talent Plans
- PRC LE to conduct covert extra-territorial activity
- Visiting scientists to transfer IP out of Canada
- Exploitation of diplomatic privileges
- Co-opting influential figures in Canada
- Strategic investment and acquisition
- Slander, defamation, or libel of targets
- INTERPOL Red Notices as a vehicle for 'Fox Hunt' activity
- Pro PRC narratives to incentivise the diaspora
- Use of tourism as a cover

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

SECRET

Targeted Technology Observed Overall

Principal target industries: agriculture, aerospace, virology, pharmaceuticals, and dual-use technologies.

22%	**Biomedical and biotechnology research** (Pharmaceutical drug research, polymers, cellular regulation, contagious diseases, animal diseases)	11%	**Aerospace** (Satellites, launch dispensing units, synthetic aperture radars)
19%	**Manufacturing** (Automotive Battery Research, industrial equipment – valves, pipeline inspection tool)	8%	**Telecommunications** (fibre-optics)
17%	**Agriculture and Food** (Seed and germplasm genetics, wheat, potato, pulse crops, forage research)	6%	**Aviation** (Aviation flight data, avionics systems)
11%	**Protected business practice and operations information**	6%	**Environmental related technology** (Meteorology - Air quality forecast modeling)

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Challenges

SCOPE

- PRC FAI activity crosses multiple RCMP FP business lines (Cyber, SOC, BI) impacting visibility.
- Lack of reporting by private industry due to fear of economic losses or impacts to operations and reputation.
- Underreporting by victims due to fear of retribution.

INVESTIGATIONS

- Intelligence-led investigations and caveated information.
- Complexity of investigations is high and requires subject matter expertise.
- Attribution to State actors is difficult to prove.
- Technology and OPSEC requirements

LEGAL & GOVERNMENT

- Political will is required to effectively address the issue: whole of GoC commitment and approach.
- Consequence management is a significant consideration given historical incidents.
- What is legal vs illegal activity?
- Legislative gaps – difficulty in applying offences.

Questions?

Slide Notes

Slide 1:
Welcoming Remarks

Slide 3:
We categorize FAI activity into target areas. These are the broad categories of FAI activities.

There are no neat buckets; Overlap in between the categories.

For the purpose of the analysis, we identified the category that best reflects each individual investigation/file.

Slide 4:
Examples include:

Slide 5:

Examples include:

Democratic Institutions:
FAI in IMVE
Freedom Convoy
Disinformation of UFWD – anti-Asian

Slide 6:
145 files (from 2011 to 2022)

Convictions:

2014-2004
Su BIN
Conspiracy to Gain Unauthorized Access to Protected Computers (U.S. indictment)
Gaining Unauthorized Access to Protected Computers (U.S. indictment)

2014-162207 (PROS) Project OSENSOR
Arthur PANG
1 x Failing to report exported good having a value exceeding $2000.00 contrary to SS. 95 and 160 of the Customs Act (Pled guilty pre-trial)
1 x Exporting or transferring goods included in an Export Control List wihtout an Export Permit contrary to ss. 13 and 19 of the Export and Import Permits Act. (Pled guilty pre-trial)

2011-734 Project SENTIMENTAL
Klaus NIELSEN
10 counts relating to offences under the Human Pathogens and Toxins Act, the Export and Import Permits Act, and the Transportation of Dangerous Goods Act

2017-2318
Li GANG
1 x Section 16(1) of the Health of Animals Act
1 x Section 51(a) of the Health of Animals Regulations

Files with current charges:

2022-1219
Yuesheng WANG (Hydro Québec)
1 x 19 (1)(b) (2) SOIA
1 x Fraudulently use computer 342.1(1)(a) cc
1 x Trade Secrets sec 391(1)(2)(3) cc
1 x Breach of trust sec 122 cc

2011-734 Project SENTIMENTAL
Weiling YU
1 x Breach of Trust by Public Officer; Outstanding endorsed warrant of arrest (Ontario Only)

2018-78;
Yantai GAN
1 x Breach of Trust by public officer sec 122 CC (Stayed – R v Jordan)
1 x Possession of property obtained by crime sec 354(1) (Stayed – R v Jordan)
1 x Fraud sec 380(1) (Stayed – R v Jordan)

2013-5122 Project SEASCAPE;
Qing Quentin HUANG
2 x Par. 16(1) SOIA - Stayed (R. vs. Jordan)
2 x Par. 22(1)(C) SOIA – Stayed (R. vs. Jordan)

2019-2117
Wanping ZHENG
1 x Breach of trust by public officer sec 122 CC

Charge Packages in progress:

2020-351
[redacted] aka [redacted] (Draft RTCC)
2 x Fraud sec 380(1)(a) CC
1 x Forgery sec 366(1) CC

[redacted]

(These charges were dropped and investigation to be concluded as of June 2022) 2020-1387 Gonzalo RODRIGUEZ
1 x Unauthorized use of computer sec 342.1(1) CC
1 x Trade Secret sec 391(1) CC

Slide 7:
145 files

The RCMP is largely dependent upon International Law Enforcement (Solely represented in the data by), followed by public complaints, and the GoC in 4th for referrals to the RCMP for the initiation of investigations involving PRC-FAI.

GoC departments: AAFC, PHAC, CSA, CFIA, etc.

Challenge: Almost a quarter of referrals from public. The reliability of information cannot be confirmed.

Notably gaps include reporting from private companies, municipal police and academic institutions > opportunities for engagement to bridge reporting gap with outside stakeholders

83% of files generated by information/complaints received from outside the RCMP:

23% International Law Enforcement (Only in dataset)
23% Public complaint/tip
18% RCMP generated – Referrals from other RCMP business lines in HQ, from divisions or within FPNS
16% of files come from referrals from other branches of Canadian Government namely: AAFC, PHAC, Canadian Space Agency. The agencies are considered victim agencies/complainant.
10% Other Canadian agencies – CSIS, FINTRAC, CBSA (CBSA key partner)
5% Domestic Law Enforcement
1% Private company
1% Academic Institutions
3% International organization – ICAO

Slide 8:
2023 trending upwards 60% expected increase

Divisional distribution highlights: E (24%), O (23%), C (10%), K (9%)

NHQ files (27%) if asked.

Pre-2018, not an indicator that these files or activities didn't exist.

2012: 0 files
2015: 0 files

Year over Year % change
2011: N/A
2013: 100%
2014: 50%
2016: -33%
2017: 50%
2018: 233%
2019: 10%
2020: 73%
2021: 132%
2022: 14%
2023: projected 60% increase

Slide 9:
145 files

1 Target Area assigned per file

Noted increase of Transnational Repression (TNR) files in 2022 (Chinese overseas police stations, Fox Hunt, targeting of 'five poisons' groups)

Target Areas: Divisional Transnational Repression (TNR) and Theft of Intellectual Property (TIP)
E – TNR 66% of files, TIP 3% of files. Note: Critical Infrastructure 17% (2nd highest target area in E Division)
O – TNR 33%, TIP 27%
C – TNR 20%, TIP 20%, Note: Theft of Protected Information 20% (tied with other two main target areas)
K – TNR 33%, TIP 25%

One file can fall into multiple categories of FAI target area activities

Slide 10:
145 files

Not an exhaustive list of TTPs. List being updated as analysis identifies patterns, new TTPs being used.

TTPs illustrate a wide range of tactics and tradecraft used to conduct FAI activities.

TTPs used against GoC: Cyber for theft of IP and/or PI, Strategic Placement, and Talent Plans (recruitment of researchers)

Threat, violence, intimidation, or coercion of family and associates in Canada and/or the PRC: a very powerful lever used by PRC. Victims and witnesses not willing to come forward. Observed in most TNR files. Difficulty in Canadian authorities to protect family and associates abroad.

Slide 11:
Drawn from dataset of 145 files

Observed targeted technologies: Drawn from 36 files in dataset involving transfer, acquisition, and theft of technology.

Collection efforts by the PRC are aligned with the research and technologies outlined in the CCP's Five Year Plans as well as the Ten Year Plan "Made in China 2025".

Slide 12:
Considerations and Key Takeaways

Who is best placed to disrupt the threat? Prosecution and criminal charges do not necessarily need to be the goal or the outcome.

Lack of identified perpetrators in Canada and limitations in legislation highlight the need for increased collaboration with partners to effect disruptions and other Threat Reduction Measures (TRMs).

Continued and increased partner engagement, including across RCMP internal business lines and with Police of Jurisdiction (PoJ), will be key to early threat identification.

Information and evidence collected by the RCMP may be unique information and can be leveraged by intelligence agencies in support of their respective mandates to augment the intelligence picture, produce additional reporting and identify opportunities for disruption.

SCOPE
PRC FAI activity crosses multiple FP business lines (Cyber, SOC, SII).
Lack of reporting by private industry due to fear of economic losses, or impacts to operations and reputation is limiting our understanding of the PRC FAI landscape.
Underreporting by complainants (victims, agencies etc..)

Legislative gaps – difficulty in proving SOIA offences
Intelligence to evidence barrier
Lack of reporting – RCMP investigations dependant on caveated partner information
Underreporting by complainants/victims – engagement required
Reluctance of victims/witnesses to come forward and act as witnesses due to fear of retaliation
Political sensitivity and complexity of investigations
Thinking outside the box – Section 83 always paradigm
Lengthy court proceedings
Reluctance by victim to report in timely manner and internal investigations conducted
Delays in investigation due to large volume of documents to review/translate
Complexity of subject matter and need for SMEs
WeChat
Comsec and Opsec

NOTE *****PRC-FAI activity crosses RCMP business lines and FPNS does not have oversight/governance of these areas.

Attribution to state actors difficult (Clandestine and covert tradecraft, etc)

Previously in slide:
PRC FAI activity crosses multiple FP business lines (Cyber, SOC, SII).
Lack of reporting by private industry due to education, fear of economic losses, or impacts to operations and reputation; is likely limiting our understanding of the PRC FAI intelligence landscape.
Legislative gaps – difficulty in applying offences
What is legal vs illegal activity?
Early identification of potential threats
Underreporting by complainants (victims, agencies etc..)
RCMP investigations dependant on caveated partner information
Political sensitivity and complexity of investigations
OPSEC requirements
Technological challenges: Use of encrypted communications
Attribution to state actors difficult

Political appetite
Deconfliction focus instead of collaboration

Slide 13:
Closing remarks