

OLD THREATS, NEW THEATRES: SECURITY AND INTELLIGENCE IN THE DIGITAL AGE

November 4,
2022



Supported by:



This report is based on the views expressed during an annual symposium organized by the Canadian Association for Security and Intelligence Studies. Offered as a means to support ongoing discussion on security and intelligence issues, the report does not constitute an analytical document nor represent any formal position of the organizations involved.

<https://casis-acers.ca>

Report by Annabel Zhu, Syed Shaan-e-Ali Mehdi

© 2022 CASIS-ACERS. All Rights Reserved.

CANADIAN ASSOCIATION FOR SECURITY AND INTELLIGENCE STUDIES

Who We Are

The Canadian Association for Security and Intelligence Studies (CASIS) is a nonpartisan, voluntary organization established in 1985. Its purpose is to provide informed debate on security and intelligence issues in Canada. A distinguished board of directors comprises professionals of national and international reputation and status who oversee the association's operations.

Membership is open and includes academics, government officials, lawyers, former intelligence officers, students, and interested members of the public committed to the study of security and intelligence.

What We Do

For over twenty-five years, CASIS has held an annual meeting and has sponsored conferences, symposia, and fora on intelligence and security-related themes. The first conference was held at Glendon College in Toronto in June 1984, with others being held in Vancouver, Montreal, Calgary, and Halifax; more recently, annual conferences have been held in Ottawa.

OLD THREATS, NEW THEATRES: SECURITY AND INTELLIGENCE IN THE DIGITAL AGE

 CASIS-ACERS

20
22

TABLE OF CONTENTS

Keynote: How to Lose the Information War: Perspective from the US and Beyond	6
Panel: Financial Wars – New Economic Warfare	8
Presentation: CASIS Essay Competition Winners	11
Panel: Bridging the Private-Public Sector Intelligence Divide	13
Fireside Chat: Disinformation, Misinformation, and Information Operations – Implications for Canada and Partners	16
Panel: Digital Authoritarianism and the Future of Electronic Surveillance	18



KEYNOTE NINA JANKOWICZ

The threats that disinformation campaigns present to democracies do not occur in a vacuum. The intentionally false or distorted information flowing out of places like Russia and aimed at nations from the U.S. to Eastern Europe is part of a more significant effort to prey upon existing societal divisions, especially within democratic societies. For that reason, a nation's strategy to counter bots, online trolls, and outright lies must go together with a robust civic renewal effort.




Case study: The United States

We believe that the pandemic is taking part in this backdrop. Even though it has ended, the after-effects of the pandemic are making it more difficult to address the issue of disinformation. Most customers are currently comfortable in buying things online which has increased the potential for online disinformation campaigns by adversaries to be used more frequently.

Western democracy is currently facing dual crises of truth and trust. Since Putin came to power two decades ago, the United States and the West have been under attack in the information war, whether they want to acknowledge it or not. The United States failed to establish itself as a leader in the struggle to uphold democracy.

- Online information operations have also become more diffuse and sophisticated, adapting their tactics to increased scrutiny rather than simply creating fake accounts and information.
- The U.S. government needs to invest in building public awareness of disinformation. Disinformation campaigns weaponize citizens' emotions. Fighting against disinformation requires widespread digital literacy campaigns targeted at voters and social media users as well as involving politicians, civil servants, and public relations professionals.



Jankowicz's individual experience demonstrates how the U.S. government still does not take this problem seriously and how partisan disinformation undermines democracy and inspires hate for fellow citizens.



Case Study: the Czech Republic

There is an essential role for individuals in encountering and mitigating disinformation and working to repair polarization. The story of the disinformation campaign which created propaganda against the EU and migrants in the Czech Republic should be a warning to governments in the West.

- The Czech government created the first unilateral government body to counter disinformation but faced much criticism from their president and the public. Nevertheless, the case study of the Czech Republic taught the world the importance of developing systemic and generational solutions.
- The most egregious mistake Western governments have made is assuming that the information war is just about information. It's much more pressing than that; it's about the future of democracy itself. Even if the attacks are primarily digital, their effects live in the real world.



Where do we go from here?

Jankowicz suggests communicating actively, proactively, plainly, and transparently about efforts to counter disinformation. The government must identify the source of online disinformation campaigns and be ready to back its public servants and public-facing employees. Not only defending their expert records but anticipating and planning for online attacks that lead into offline spaces.

Citizens-based solutions: governments and private sector investments in media, digital literacy, civics, cyber hygiene, and essential awareness.

- Beware of the vector of homegrown disinformation.
- Leaders must recognize we cannot fight external disinformation when it is a problem domestically as well.

Panel 1: Financial Wars – New Economic Warfare

Rachel Ziemba

Financial sanctions and targets are increasingly being relied upon such as travel bans, the use of the extraterritorial power of the American financial system, and import bans.

Case Study: Russia

- This set of economic tools as economic pressures are happening at a time where there is an inter-state war. In Russia, the ongoing war against Ukraine changes the context.
- Coordination matters. Having a broad coalition deepens the impact and increases over-compliance.
- The agency of the target really matters. This is true for the Russian as well as Iranian contexts. Actors we are trying to disempower become stronger in their domestic context. It may not always be avoidable so we should assume that this might happen.
- The agency of alternate countries matters. Alternate supply chains and payment channels might open up through countries that are willing to operate in the grey area.
- It is hard to maintain large sanctions programs and conduct economic warfare on many countries at the same time. It is important for us to take more time thinking about implementation impacts and discontinuities and shore up domestic financial systems.



Michael-John Almon

What Is FINTRAC?

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has a dual role as both the regulator for Canada's anti-money laundering and anti-terrorist financing regime and also as Canada's financial intelligence unit.

- The links between money laundering and terrorist financing are vital and these aspects touch many different parts of financial transactions and national security.
- The rise of cryptocurrency being used as a crowd-funding measure through social media has the potential to be both the most over-rated and under-rated aspect of financial intelligence. It is imperative to understand it better to improve visibility on all types of customer transactions taking place in the financial intelligence space.
- The financial intelligence realm is very collaborative, perhaps more so than other fields of intelligence. With regards to money laundering and terrorist financing, it isn't just FINTRAC that is involved, there is a very large regime of multiple agencies that are involved in the federal, legal and information reporting spaces. Information from all these different quarters comes to FINTRAC and it is packaged with the end goal of keeping everyone safe by trying to understand how threat actors may misuse and abuse the financial system. Ultimately it is a large collection of varying organizations, both in the public and private sphere, that are working together.



Mario Cosby

How is crypto used in economic warfare?

The actors are still the same but the weapons have changed. Crypto crime and financial crime are the same but the tools have changed as we now have a new weapon.

How do we combat this new weapon?

These negative actors have to be stopped from moving from the crypto space to the traditional financial space - this is where blockchain intelligence comes into relevancy.

Use of blockchain intelligence in the form of defensive capabilities:

- Using blockchain intelligence for transaction monitoring.
- Wallet screening.

Use of blockchain intelligence in the form of offensive capabilities:

- Following the money is crucial and blockchain can be used to accomplish this in the form of blockchain tracing.
- More dark-net markets can be shut down.

“Do not ignore crypto crime, it is still financial crime at the end of the day. While it is a new weapon used by illicit actors, there is also a new weapon to counter it, which is blockchain intelligence.”

CASIS Essay Competition Winners:

LEUVAN WONG: THE DISINFORMATION CASE FOR A NEW APPROACH TO CANADIAN INTELLIGENCE

States can use disinformation to further their agendas by changing how society views military interventions and by building communities of like-minded individuals. “Naturalization”, which is the projecting of a counter-narrative towards foreign audiences without contrasting it with the opposing narrative, aims to act as a defense against disinformation campaigns by highlighting what values and systems are worthy of emulation.

Two Proposed Changes to Naturalization:

- 1) Naturalization should be more oriented toward the domestic audience.
- 2) The counter-narrative has to be true. It is not enough to project a counter-narrative; hence, the narrative has to be factual to separate Canada from the rest.

What are the benefits of this approach?



- 1) This solution is compatible with our democracy and ensures that our response to disinformation preserves democratic debate by minimizing the need to block opposing narratives.
- 2) This allows the government to plan national security strategically.
- 3) Most importantly, it fights disinformation. Using an alternative narrative to fight foreign disinformation narratives will be even more effective if the report is accurate.
- 4) Opens new ways to learn about and combat disinformation, including through partnerships with other agencies, NGOs, and businesses.

Conclusion: This is a new way to think about national security, which makes it more comprehensive and helpful towards the ongoing mission of making Canada stronger and each Canadian freer.

CYBER ESPIONAGE IS HERE TO STAY: A REALIST APPROACH TO CYBERSECURITY

Paige Smith

States' vested interests in information gathering will inhibit the collective adoption of international regulatory policy for cybersecurity.

States are attracted to cyber espionage because of its low cost and covertness that allows them to attain valuable information without disclosing their intentions to the target.

Even though there have been attempts to define what international law applies to cyberspace, these still need to provide adequate details or achieve a consensus on a global scale.

Smith argued that the international system is constantly in a state of anarchy, and conditions are motivated by self-interest and to gain greater power.

Two Potential Solutions:



Establish International Norms

Maintain Exclusivity in Cyber Policies

Conclusion

In cybersecurity's power-seeking and chaotic political climate, it is challenging to advocate for more stringent cyber regulation and establish legal frameworks to hold nations accountable. Large countries will probably continue to develop a more impressive cyber arsenal to keep their competitive advantage while spying on adversaries to assess their capabilities.



Panel 2: Bridging the Private-Public Sector Intelligence Divide

Dr. Maria Robson Morrow

There are three main ways by which public and private sector intelligence interact: Firstly, they work together in the field of government outsourcing such as private sector intelligence and security companies providing services to the government. Secondly, they work together in the fields of corporate espionage; and thirdly, they interact through competitor and business intelligence mechanisms.

Moreover, 57% of intelligence professionals had a government background while 43% did not. This is a different statistic than what we would have seen 20 years ago. Previously it was almost required to have a government background to get into intelligence however today people can come directly from the private sector.

3 Key Takeaways

- 1) Private sector intelligence professionals are everywhere. This is a growing field in terms of the number of people involved as well as scope of what these professionals are doing be it strategically or tactically. These are potential partners who are motivated with national security and want to assist the government but often don't have the mechanisms to do so. They are building their own mechanisms for cooperation regardless of what happens on the government side.
- 2) There are good public-private models out there that serve to inform Canadian initiatives.
- 3) Academia, intelligence and security studies should be incorporating the existence of intelligence in the private sector.





Ryan Long

3 Recent Trends in Private Intelligence:

- 1) Historically, the field primarily existed of subject-matter experts who had deep expertise on certain topics or geographic areas, who would produce as many intelligence products as possible. This has evolved into more of strategic advisory role that is working side by side with the public side and framing intelligence as an end-to-end, consumer focused service.
- 2) The focus has gravitated away from specific threats, whether it be threats to executives or other employees, to providing advice on strategic decisions.
- 3) The scope has expanded for different fields in the private intelligence sector, such as law.

EVOLUTION OF PUBLIC-PRIVATE INTELLIGENCE PARTNERSHIPS:

At first the relationship was transactional. Today, rather than just sharing intelligence, it has extended to forming real partnerships and relationships.

Intelligence is a team sport and requires the active participation of everyone involved to really make it effective. The current trend of increased collaboration has made a big difference. However, this is a personal endeavour. Meaningful connections must be built in order for trust to form, so critical and time-sensitive information can be shared effectively. This is becoming more common.

The Overseas Security Advisory Council (OSAC) can be considered a gold-standard in public-private intelligence partnerships. Another example is the Analytic Exchange Program in the US in which analysts in the public and private sectors get together and work on the most challenging national security related issues that the nation is facing.

DR. PIERRE-LUC POMERLEAU

There are many crises that we are facing. For example, prior to 2015 it was possible for banks to share information among themselves about any types of threats such as physical, cyber or fraud. That is not the case today.

- The legal landscape is fairly complicated, there are a lot of privacy laws to navigate at both the provincial and federal levels.
- Compared to the US' *Patriot Act*, there is no such mechanism in Canada that allows organizations to share information between themselves as well as with the public sector.
- There is an issue with reciprocity. In other words, if information is shared, will it be shared in return so that internal processes within the protection mechanisms can be improved.
- There is no platform to share information in a secure manner. For example, it is critical that banks protect customer information; but if there is no platform to share information securely, then that becomes an issue.
- There were conflicting organizational missions and objectives. For example, law enforcement agencies want to make arrests while the private sector wants to reduce fraud losses.

Key takeaways

- The role of interpersonal relationships is vital in sharing information and can take the place of sharing information on certain platforms.
- One of the gold standard public-private organizations that was uncovered from the research is the National Cyber-Forensics & Training Alliance (NCFTA) in Pittsburgh. This is a tactical partnership that focuses more on cyber fraud and financial crime. For example, the FBI will work with banks in the same office and share information on a daily basis on the same platforms.
- Between 2015 and 2021, there were 4,184 cases that were referred to law enforcement by the NCFTA. More than 26,000 intelligence reports were produced, 1,179 arrests were made and more than \$12 billion in lawsuits was prevented.
- Another gold-standard organization is in Australia called the Fintel Alliance. This partnership started in 2017 and now has 29 organizations under its ambit. Their goal is to share information to prevent money laundering and terrorist financing.
- The concept of sharing information in real time, working under the same roof and working directly with one another on the same platforms is vital in ensuring the effectiveness of public-private partnerships in the intelligence field.



FIRESIDE CHAT: DISINFORMATION, MISINFORMATION, AND INFORMATION OPERATIONS: IMPLICATIONS FOR CANADA AND PARTNERS

Dr. Stephanie Carvin

- Be aware of the power of disinformation. It is important to not overly secure the information space as it is crucial for democracy.
- Nowadays, more actors are involved in disinformation. As a result, we live in a world of misinformation, disinformation, and propaganda impacting our real lives and political elections.
- It has been an ongoing issue. Actors such as states and non-state entities using disinformation tactics can result in destabilization. Democracy is then vulnerable because it's based on the foundation of open speech and sharing ideas. Citizens need to be extremely cautious to avoid becoming the targets of misinformation.
- Political disinformation campaigns using misleading narratives are also present in Canada. CSIS is Canada's domestic national security intelligence service, mandated to collect information "within or relating to" threats to the security of Canada. These are defined as espionage, foreign-influenced activities, terrorism, and subversion.
- Another concern regarding misinformation is that foreign states purposely expose themselves with a goal to discredit the electoral processes in various places. Eg: News about Russian interference in Western election cycles may be intentionally released by Russia since it casts a shadow on and pushes people away from the overall democratic process.

class": "com.orgmanager.handlers.RequestH
eChars": "5022", "message": "Durati
BURL": "/app/page/analyze"
+ID": "824000"



Marcus Kolga

Russian state media has brazenly manufactured facts and evidence, including mock interviews and photos, to promote its viewpoints throughout its war with Ukraine.

- Canada has also been the victim of disinformation. Recent disinformation about the Canadian Armed Forces in Latvia provides a raw example of the crudeness of disinformation campaigns. In one case, Defence Minister Harjit Sajjan's appearance, including his turban, was exploited by pro-Kremlin media to stoke racist sentiments.
- Governments must start by recognizing that our democracy is being targeted when creating tactics and policies to counteract foreign misinformation. The Kremlin is presently waging a full-scale information war against Canada and its allies to negatively impact our societies and undermine our faith in our leaders, the media, and one another. Therefore, Canada's reaction must be forceful and must consider all channels through which foreign media warfare is carried out. Most significantly, we need to be ready for a protracted battle.

Looking forward

The best defense against propaganda and misinformation is media literacy. To encourage increased critical thinking among all Canadians when consuming information, Canada needs a national media literacy plan.

Public service announcements must be created to describe how to spot false information, the websites that spread it, and the dangers of using social media as a primary news source.

PANEL 4: DIGITAL AUTHORITARIANISM AND THE FUTURE OF ELECTRONIC SURVEILLANCE

Dr. Leah West

- To think of national security as the basis for human rights is hazardous. In times of crisis, governments may use this logic to suppress, restrict, or destroy individual rights and liberties. Significant international and local law has been established to prevent the denial of rights in the guise of crises affecting national security.
- A population does not lose the protection of their universal human rights simply by living in a state involved in a conflict, or subject to occupation.
- The desire of a military or other security force to access all data and information, and leverage it to satisfy their responsibilities under the precautionary principle, cannot be above the privacy rights of an entire population. A population's human rights do not dissipate entirely because of the needs of an occupying or defensive armed force.
- States need to develop policies that can reflect privacy principles involving data protection laws as well as state, domestic, and regional protection obligations.



How social media reinforces threats

Social media platforms can be used to facilitate surveillance of international users; the platforms' algorithms could be configured to censor content or to conduct imperceptible influence operations.



Western governments around the world have historically segregated cyber threats based on this information. Western governments have advocated for an open multilateral system and developed internet standards such as the T Protocol.



The internet is lacking in solid authentication; this is a serious issue because it facilitates the split of information. Any positions adopted by the Canadian government must recognize that threat actors search for product vulnerabilities with little care for where those products are developed or produced.



Only by broadly improving the security integrated into contemporary technologies will everyone in Canada be made safer than they are now from foreign and domestic operators who are working contrary to Canada's domestic and foreign interests.

AKSHAY SINGH

1

Leaders with authoritarian tendencies engage in "digital authoritarianism" and rely on the internet and related technology. This decreases trust in public institutions, increases social and political control, and/or undermines civil liberties.

2

Digital tools can be used to democratize and spread information freely, rather than limiting rights and preventing conversations on problematic topics in certain countries. The concept of data sovereignty is challenging for countries as it can be cost-prohibitive.

3

Some states invest heavily in data and internet systems, and view technology as a repressive tool. These countries will be using technology to stifle and push state narratives or surveil their nationals resulting in an increased risk of people being perpetually controlled.

4

Democracy is highly vulnerable; countries that have heavy control over data and the internet create an uneven playing field in terms of people's ability to access information and give governments a way they can control that data further. This technology can be proliferated to other regimes that are also repressive.



THANK YOU



CASIS-ACERS