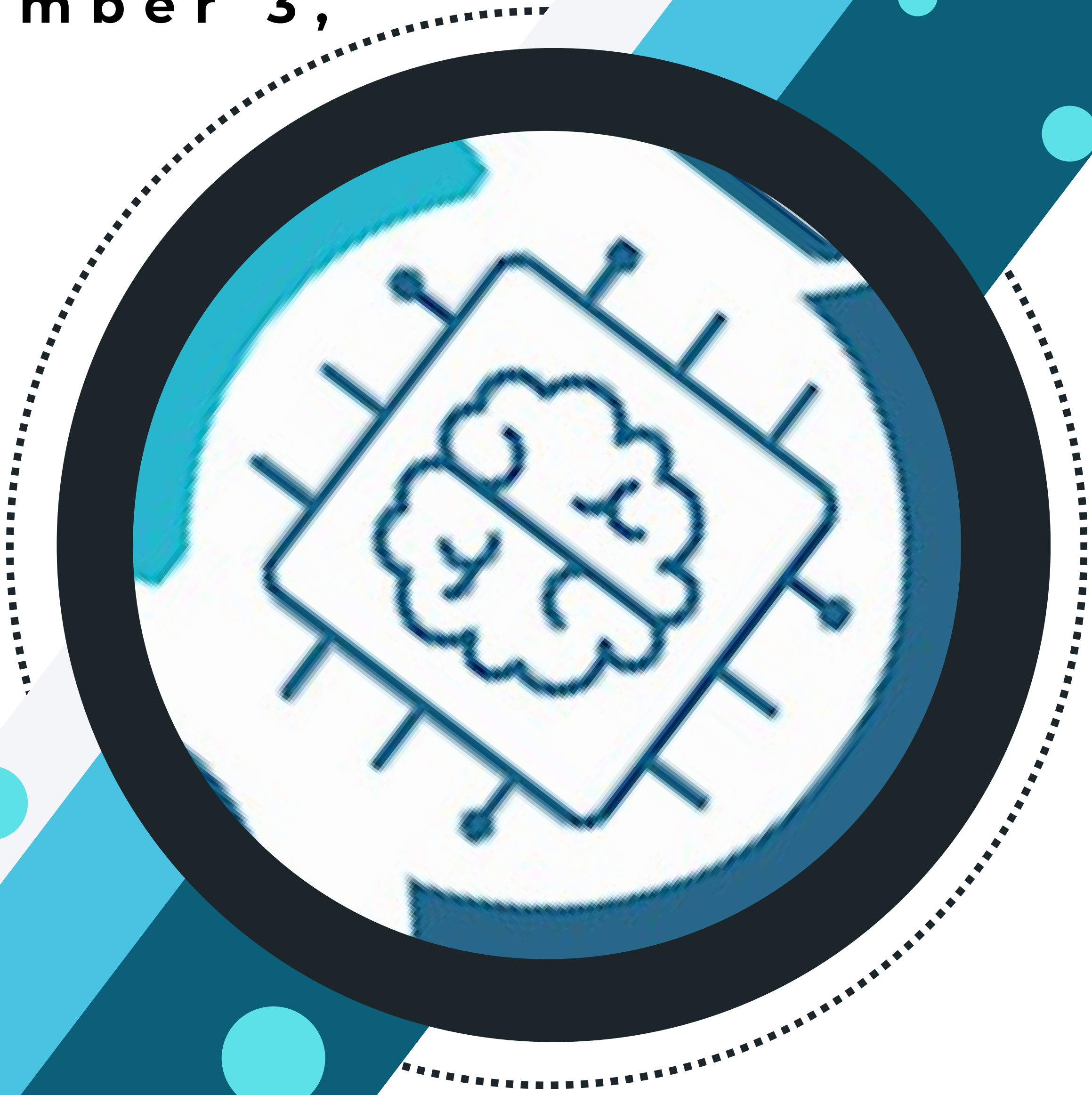
THE FUTURE OF INTELLIGENCE IN A POST-TRUTH WORLD

November 3, 2023



CASIS-ACERS

Supported by:

MINDS
MOBILIZING INSIGHTS IN DEFENCE AND SECURITY

FINTRAC CANAFE
Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

uOttawa
Institut de développement professionnel
Professional Development Institute

tada web

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 Syed Shaan-e-Ali Mehdi

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

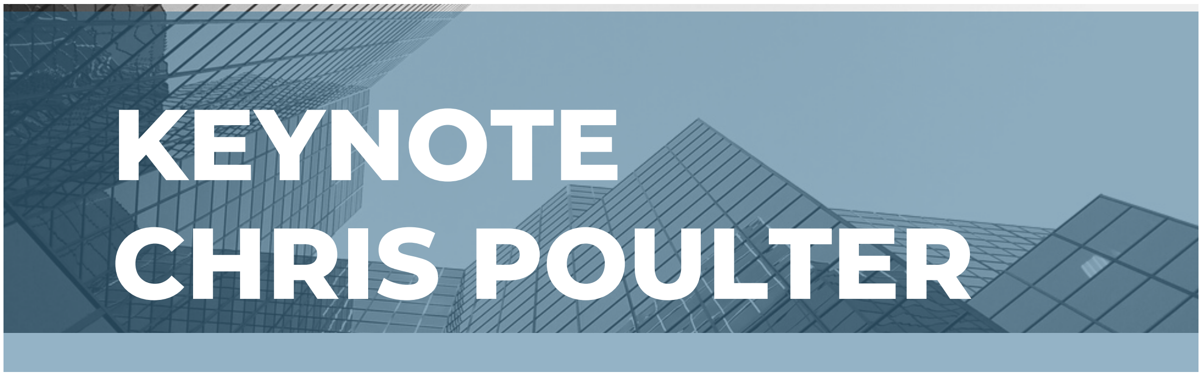
For over twenty-five years, CASIS has held an annual meeting and has sponsored conferences, symposia, and fora on intelligence and security-related themes. The first conference was held at Glendon College in Toronto in June 1984, with others being held in Vancouver, Montreal, Calgary, and Halifax; more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

THE FUTURE OF INTELLIGENCE IN A POST-TRUTH WORLD

CASIS-ACERS

2023

TABLE OF CONTENTS



KEYNOTE CHRIS POULTER

OSINT AND AI: UNDERSTANDING OSINT WITH EMERGING TECHNOLOGIES AND THREATS

What is OSINT and what value does it bring?

Open-source intelligence (OSINT) is the collection, processing & analysis of publicly available information to answer a specified intelligence question. OSINT sources are vast and the key is to figure out how to sift through them to find value.

One key takeaway from the advent of OSINT is that intelligence does not have to be secret to be valuable. When used in tandem with classified information, OSINT can offer its full utility to the field of intelligence.

Examples of the different roles and uses for OSINT:

- Social listening and situational awareness (e.g. trends, news, etc.)
- Investigating digital footprints to identify subjects of interest or targets
- Supporting targeting measures, when combined with other forms of intelligence
- Informing response and recovery efforts by (e.g. geolocation, weather data, local social media accounts, image analysis, etc.)

The POLE-AE (person, organization, location, event, action and equipment) data model provides a basic set of principles to guide OSINT activities.

Developing OSINT Capability: Steps for Success

- Executive influence and buy-in: the executive level needs to support and understand the value of OSINT.
- Organizational alignment: OSINT activities need to align with internal factors such as legal boundaries, mandate, accountability, priorities, and policies.
- Understand existing capabilities and needs: an organization must grasp personnel skills and knowledge, consult the range of free and commercial tools that are available, and identify the types of data that are being sought.
- Define the end-state: identify the desired value that OSINT activities and capabilities will facilitate or provide, and consider who will be affected.

Using OSINT for tactical and strategic purposes

- Threat landscape: OSINT can provide a comprehensive picture of a given threat environment, particularly when assessments are corroborated and reviewed against other forms of intelligence.
- Personnel security: social media accounts and geolocation tools can validate if personnel are safe, although adversaries can also exploit the same forms of data.
- Investigations: OSINT can aggregate disparate forms of publicly available information to identify threat actors and develop profiles.
- Humanitarian sphere: OSINT can be used to identify viable routes for exfiltration during natural disasters or conflict.

How Does Generative AI Help The Field of Intelligence

- Lowers barriers to entry across disciplines (condenses manual research)
- Interrogates complex and comprehensive data sets
- Lowers barriers to data interrogation: human asks question, program organizes and formats data in digestible format with which the human can derive meaning - even with little prior knowledge or expertise
- Existing approach vs generative AI approach (Analyst asks question and AI produces product)
- Validating the information returned is still critical: the analyst’s role is to scrutinize information against knowledge, identify potential biases or gaps, and corroborate findings against other sources

ChatGPT and Challenges to National Security

Adversaries and malicious actors can manipulate AI systems by introducing disinformation, conspiracy theories, or biased information to the datasets. These actors can also exploit existing biases in datasets, and use generative AI in propaganda or disinformation campaigns (e.g. generating racist images or fabricated texts).

Operational security, data retention, storage and privacy can be negatively impacted by AI due to poor sourcing and copyright infringement.

Panel 1: AI, Intelligence and "Truth"

Nestor Maslej, Dr. Daniel Araya, Dr. Susan Aaronson, Brad Boyd

Aligning and Adapting Our Current Systems for AI

AI is a collective term used for different technologies that are often aligned between different systems to be able to harness their potential. Developments in Artificial Intelligence (AI) have brought plenty of benefits and risks; the latter include the lack of checks and balances on information produced by tools like ChatGPT. No system is fully unbiased or contains zero risk, so the key is to align systems with human intent. This iterative process involves recurring failure and revision to achieve optimal alignment.

This technology is fast outpacing the institutional framework that was built in a different era and environment. Whereas many previous cutting edge technologies emerged from research labs in universities, the majority of AI developments have come out of industry rather than academia due to intensive capital requirements and market-based incentives.

Despite the risks and uncertainties of this emerging technology, there is growing recognition and consensus that our security, intelligence, defence, and bureaucratic systems need to more effectively adopt and leverage AI tools. For example, the U.S. Defense Advanced Research Projects Agency (DARPA) Mosaic Warfare program is one example wherein the structure has been designed to be less constrained by a slow-moving bureaucratic framework.

So what could be done to balance these issues? One way is to use the iterative process to incorporate accountability and ethical frameworks that more closely align AI systems with institutional objectives and values.

In this new multi-polar environment, China is working towards increased adaptability. Accordingly, there is a greater need to test what systems can be adaptable and ensure that we do not fall behind. Will decentralizing decision-making truly be effective?

Similarly, how can we adapt our militaries to reflect a system that emphasizes a tailored approach to operations based on threat? How can we balance flexibility and effectiveness?

The Importance of Data in AI and Intelligence

There is no AI without data. Generative AI needs data but there is a quality control issue that can affect datasets. For example, there are minimal measures in place to screen social media data for accuracy, reliability, biases, or completeness. As a result, the data obtained for developing AI tools may be inaccurate, incomplete and more representative of common opinion or biases. This effect causes some AI models to "hallucinate".

There is no data without trust. Sixty-nine nations signed onto the OECD principles of AI but only fourteen of these nations sought public comments on their AI strategies. Out of those, only four acknowledged the comments, and none actually changed their policies.

To create an environment of trust, the public has to be involved in decision-making related to AI and data policies. A human-centred approach involves engagement with average citizens during every step of AI deployment.

CASIS Essay Competition Winners: Graduate Category

GRADUATE WINNER: MICHAEL SHIRLEY

"SHADOW OF THE SUN: TRACING WAGNER DURING THE FIRST YEAR OF RUSSIA'S FULL-SCALE INVASION OF UKRAINE"

Why do nations use Private Military Contractors (PMCs) in the modern age? Would Wagner be used in Ukraine similar to how the United States used Blackwater in Iraq?

Shirley's research methods involved primarily using the Wagner official Telegram channel to find information on the Russia-Ukraine War and Wagner movements.

Shirley found that Wagner operated differently than other PMCs. Not only were they the main drivers of many Russian offensives, but they were more effective than the regular Russian army in achieving tangible results.

Early in the war, Russia had battlefield successes that were eventually stalled by Ukrainian forces. However, when Wagner entered the fray, for example in the Battle of Bakhmut, Ukrainian forces were unable to defend positions as effectively. During this battle, Wagner changed its strategy. Normally using smaller detachments of troops of not more than 10 per group, they changed this in Bakhmut by deploying a much higher number of mercenaries (anywhere from 30,000 - 80,000).

Wagner is also heavily invested in promoting its image through using tools such as music and symbols. However, this image-building still did not prevent its leader, Pregozhin, from falling out of the good graces of Putin.

The findings from this essay can provide an insight as to how PMCs can be used in warfare. The bottom line is that nations are likely to continue using PMCs in addition to formal military units. Wagner's notoriety and apparent success vis-a-vis Russian military units may also encourage nations to mimic the Wagner model.

CASIS Essay Competition Winners: Undergraduate Category

UNDERGRADUATE WINNER: MATTHEW KIEFFER

OPPORTUNITY TO ADVERSARY: CANADA-CHINA RELATIONS IN THE 21ST CENTURY

Fear dominates the Canadian relationship with China today. However, in the past, it was more centred along “opportunity”. When and why did relations sour? Did we get China wrong at some point or are there other questions we can ask? Could our relations with China also help them learn from us?

From the Canadian perspective, Pierre Trudeau’s tenure reflected a golden-age in bilateral relations, while Mulroney’s reflected the policy of “explicit continuity” seen through him being quiet on human rights. Furthermore, Chretien’s government was characterized by trade missions and a policy of non-intervention.

Harper’s government reflected a major shock to the relationship. While initially hard on China, for example by giving the Dalai Lama citizenship and having Canadian diplomats visit Tibet, by 2010 he had changed strategies to embrace warmer economic relations. The relationship at the beginning of Justin Trudeau’s tenure could be characterized as that of optimism, partly through channeling his father’s legacy. In keeping with Harper’s economic lens, Canada under Trudeau also went along the same path by joining the Asian Infrastructure Bank and further deepening economic ties.

However it has since been marred by repeated shocks since 2018-2019 (e.g. detainment of the “Michaels”), indicating that this new colder relationship is the rule rather than the exception. The deterioration of the Sino-Canada relationship was also exacerbated by growing explicit US-China competition and more aggressive power politics rhetoric, marked by a period of de-coupling and strategic competition. Therefore, Canada is stuck between “two very large elephants”.

There has been congruency in Canada but a shift in China; while a change in leadership may offer a new opportunity to improve relations, the prospects are grim without significant diplomatic efforts.

Panel 2: From Social Media to Satellite Imagery: Defining the Open Source Intelligence (OSINT) Landscape for Collection and Analysis

Dr. Thomas Juneau, Micah Clarke, and Dr. Leah West

Key Challenges

There are several challenges with regards to using OSINT in the intelligence sphere. These include political challenges about how easily we are able to discuss certain issues openly, institutional challenges of figuring out where to assign OSINT capacity within larger institutional frameworks, and cultural challenges around open source data being traditionally (and incorrectly) viewed as less valuable than classified information. There are also research challenges since the intelligence community has historically been averse to working with other communities such as universities and research institutions.

Outdated attitudes about the value of OSINT have largely dissipated as the intelligence community has increasingly embraced its potential, particularly as a crucial input alongside other forms of intelligence. The community is also much better placed to work with non-traditional partners, but further steps can be taken. One tangible - and existential - action could be to address the chronic security clearance backlog to ensure organizations are able to recruit and retain staff.

Challenges in the OSINT Environment

Data – there is less and less publicly available data, particularly data analytics tools. Social media platforms and third party analytics services now monetize their data, raising concerns that firms may seek to obtain this information through unethical or intrusive means.

Tools – Firms are effectively monetizing data analytics tools, particularly with respect to social media data, but prices for these tools are extremely high and there is limited transparency with respect to privacy implications. The intelligence community will have increasing demand for third party services as social media and messaging platforms offer privacy and encryption options by default that limit manual observation and collection activities.

LEGAL IMPLICATIONS OF OSINT: NAVIGATING UNCERTAINTY

The public sector tends to employ a self-limiting approach to OSINT activities because of Charter constraints and legal uncertainty (i.e. confusion about mandates and gaps/lagging caselaw). Conversely, the private sector tends to be less risk averse and more permissive in their interpretation of legal boundaries around privacy and data. For the public sector, maintaining a balance between security and individual rights in the OSINT context is a crucial challenge.

A pressing issue lies in the misconception that open source information (information available to the citizenry at large) is inherently public and therefore devoid of privacy protections under section 8 of the Charter and the *Privacy Act*. The courts continue to lag behind technological developments in interpreting the meaning of the privacy protections in the digital age. The resulting uncertainty can cause inadvertent privacy violations, risk aversion, or erroneous assumptions about the scope of “publicly available”.

Reasonable Expectation of Privacy is a Moving Target

It is important to note that “personal information” undergoes continuous evolution with new forms of data, while “reasonable expectation of privacy” (REP) under section 8 of the Charter is contextual and could shift based on changes in caselaw. Even when information is willingly made public by users, it doesn't always mean that the originator will cease to have REP in that data.

Nebulous privacy policies governing the use of OSINT often lack clear limits on the “scraping” and utilization of large sets of publicly available data, leaving room for differing interpretations on collection and retention practices. Complicating matters, the origin of the data becomes a critical question, especially when information is posted by third parties without prior consent or was posted publicly prior to the advent of complex data analytics tools.

Collaboration with the private sector further complicates the picture. Under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), information posted on social media is not automatically deemed publicly available, triggering potential non-compliance issues for intelligence agencies working with third party services.

As we navigate this evolving landscape, the delicate balance between safeguarding national security and respecting individual privacy rights demands a nuanced and continually evolving approach.

PANEL 3: HEARTS, MINDS, AND MISINFORMATION

DR. STEPHANIE CARVIN, CHERIE WONG, DR. SHELLY GHAI BAJAJ, AND DR. BESSMA MOMANI

Understanding narrative-building is crucial. In countering mis- dis- and malinformation (MDM), we find ourselves confronting a myriad of challenges that demand strategic insights and robust responses. There are four critical challenges shaping the landscape:

- **Lack of Agility and Speed in Response**: The struggle to respond swiftly and effectively is evident, as exemplified by challenges such as the India-Canada spat. The absence of a well-defined strategy leaves us vulnerable, with narratives slipping through the cracks.

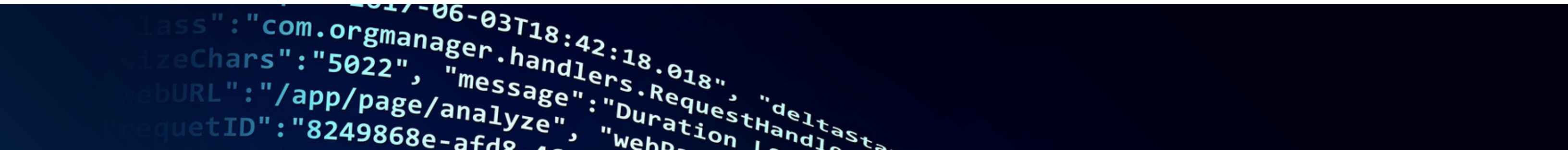
- **Lack of Institutions**: The dearth of institutions dedicated to countering MDM underscores a critical gap in our defence against evolving threats. Establishing and fortifying institutions becomes imperative to navigate this intricate battlefield.

- **Lack of Reporting**: Communication breakdowns hinder our ability to counter MDM effectively. Institutions need to enhance their reporting mechanisms, ensuring seamless dissemination of findings to mount an agile and united defence.

- **Liars' Dividend**: Bad actors exploit a compromised information environment to obscure their role in activities detrimental to truth. Lies also tend to spread more widely than the truth, which makes counter-narrative efforts more challenging.

How do diaspora communities end up being tools of MDM? Narrative discursion as a phenomenon is not confined to fake news, but includes narratives spread strategically to incite hatred. An investigation into pro-Beijing networks in Canada found that hateful narratives were disseminated through these networks, which, alarmingly, receive funding and training from state frameworks in Beijing.

While governments play a crucial role in educating and empowering citizens, the key lies in allocating more resources to ensure that diaspora communities are shielded from the harmful impacts of manipulated narratives. One proposed solution involves creating a dedicated space where individuals can fact-check news to discern its veracity. Empowering the public through information and enabling them to distinguish between truth and manipulation is deemed essential in countering the weaponization of diaspora communities.


lass":"com.orgmanager.handlers.RequestHandle
izeChars":"5022", "message":"Duration
ebURL":"/app/page/analyze", "webP
questID":"8249868e-afd8
2017-06-03T18:42:18.018", "deltasta

How Different Narratives Impact the Canadian Security Environment

MDM have a multifaceted nature, often directed at suppressing political activities from ethnic diasporas. The challenges are twofold—those we are aware of and those lurking in the shadows:

MDM in Unseen Spaces: MDM circulates on private and encrypted chat applications, traversing layered information environments. Pockets of digital nationalism from communities such as Indo-Canadians and Chinese-Canadians infiltrate Canadian spaces, creating complex narratives that ebb and flow with global events.

Changing Landscape of MDM Spread: Traditional platforms like Facebook and Twitter witnessed a decline in usage by new immigrants, with 84% of new immigrants opting for WhatsApp. Key findings reveal that these spaces serve as hubs for connection rather than information dissemination, offering unique opportunities for correction and mitigation actions.

Why Does MDM persist and thrive? Cheap, Effective, and Easy: MDM exploits divisions in a cost-effective and efficient manner, particularly from anti-Western frameworks. The oversharing of significant amounts of data facilitates exploitation.

The Future of Warfare: The shift towards exploiting cyber and other avenues of warfare is imminent, avoiding traditional foot soldier demographics. Increased connectivity and transnational communities further complicate the landscape. Moreover a poor media ecosystem in the Global South becomes a breeding ground for MDM, exploited by authoritarian leaders and a feeling of superiority, perpetuated by these populist leaders, serves as a shield against domestic failings.

Potential Solutions

Government has a role to play in educating and empowering Canadians; however, governments alone are not suited to counter these narratives. We need to respond appropriately by investing more resources towards ensuring diaspora communities are protected from harmful narratives. This could include fact-checking platforms available to the public.

PANEL 4: COVERT ACTION, DIRECT ACTION, AND FOREIGN INTERFERENCE

Dr. Benjamin Fung and Joanna Chiu

Dr. Fung's research on AI in Hong Kong heightened his awareness of the critical need for ethical considerations in AI development. As the field evolves, a more robust integration of privacy considerations into the AI development process is encouraged.

In the ongoing discourse on AI, federal-provincial collaboration emerges as a cornerstone in addressing legal intricacies in international collaboration. For example, Chinese students embarking upon degrees overseas — including at Canadian universities — are bound by an agreement that prohibits them from breaking Chinese laws, even while abroad. In the event of a breach, the family is held responsible for repaying the entire scholarship. It is important for academic institutions to understand this nuance and its implications.

The Canadian Context

Foreign interference is not a novel phenomenon in Canada, with many nations viewing those activities as a routine aspect of state-to-state interactions. This perception starkly contrasts with the Canadian perspective, where interference is distinguished from influence normally exerted through diplomatic relations.

A distinct feature of foreign interference in Canada lies in its broad reach, extending beyond vulnerable diaspora communities to encompass other, non-diaspora Canadians in positions of influence. An illustrative case involves a candidate running for city council in a small Ontario town who received an email invitation from the Chinese government, offering an all-expenses-paid trip to China to learn about the New Silk Road project.

This exemplifies China's unique, strategic approach to foreign interference, setting it apart from methods employed by other nations like Russia and India. China's methodology is rooted in the belief that foreign interference is crucial for the survival of the Chinese Communist Party (CCP). This perspective shapes their engagement with various segments of the Canadian population including federal, provincial, territorial, municipal, Indigenous, and non-governmental bodies.

Looking Ahead

In contrast to common assumptions that the Chinese population would not revolt against the CCP, recent events challenge this notion. Thousands of people protesting against COVID measures, an unprecedented occurrence, suggests that the situation may be more complex and dynamic than previously believed.

As we navigate the intricate landscape of foreign interference in Canada, understanding these nuanced dynamics is essential for developing effective strategies and safeguarding the integrity of Canadian institutions.

THANK YOU

This event would not be possible without the generosity of our supporters. We thank the Department of National Defence's Mobilizing Insights in Defence and Security (MINDS) program, Financial Transactions and Reports Analysis Centre of Canada, the Canadian Security Intelligence Service, uOttawa Professional Development Institute, and TadaWeb for their support!

MINDS
MOBILIZING INSIGHTS IN DEFENCE AND SECURITY

FINTRAC CANAFE
Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

uOttawa
Institut de développement professionnel
Professional Development Institute

tada web